LANDTAG DES SAARLANDES

12. Wahlperiode

Drucksache 12/860
14.05.2003

NEUNZEHNTER BERICHT

über die Tätigkeit des Landesbeauftragten für Datenschutz

gemäß § 27 des Saarländischen Gesetzes

zum Schutz personenbezogener Daten

Berichtszeitraum: 2001 und 2002

Ausgegeben: 28.05.2003

Inhaltsverzeichnis

1 Allgemeines

1.1 25 Jahre Datenschutz im Saarland

Der von mir vorgelegte Tätigkeitsbericht blickt nicht nur auf den ihm zugrunde liegenden Berichtszeitraum, es sind die Jahre 2001 und 2002, zurück, sondern gibt Anlass und Gelegenheit, ein Vierteljahrhundert institutionalisierten Datenschutzes im Saarland Revue passieren zu lassen. Für mich persönlich, der ich gerade mal ein wenig mehr als das erste Jahr meiner Amtszeit hinter mich gebracht habe, gibt dieser Bericht aber auch Anlass, einen Rückblick auf die Tätigkeit meiner Vorgänger im Amt des Landesbeauftragten für Datenschutz des Saarlandes zu wagen.

Gerade diese Rückschau hatte für mich einen besonderen Reiz. Gab sie mir doch nicht nur Gelegenheit, mich eingehend mit der Arbeit der bisherigen Landesbeauftragten zu befassen, sondern auch mit der der bisherigen Landesregierungen und vor allem auch mit der – nicht nur auf dem Gebiet des Datenschutzes - gesetzgeberischen Tätigkeit des Saarländischen Landtages in seinen verschiedenen Wahlperioden und damit in seinen unterschiedlichsten Zusammensetzungen. In ihrer Gesamtheit gesehen ermöglichte mir diese Rückschau zudem einen tiefen Einblick in ein Stück Geschichte unseres Saarlandes.

Leider würde es an dieser Stelle den gesetzten Rahmen bei weitem sprengen, so auf die Historie des Datenschutzes – nicht nur hier im Saarland – einzugehen, wie ich dies persönlich gern täte – und wie es der Bedeutung der Materie auch entspräche.

Nicht wenigstens im Ansatz einen kurzen Abriss der Entwicklung des Datenschutzes im Saarland in den letzten 25 Jahren gegeben zu haben, wäre indes unverzeihlich.

Nun, in diesem Zusammenhang gilt es gleich zu Beginn der Ausführungen der sehr weit verbreiteten Fehlvorstellung zu begegnen, institutionalisierter Datenschutz – manche meinen sogar Datenschutz überhaupt – gäbe es erst seit dem Tage im Dezember 1983, an dem das Bundesverfassungsgericht sein berühmtes und immer wieder – auch und gerade für Kenner der Materie - lesenswertes Volkszählungsurteil verkündete (Urteil vom 15. Dezember 1983, BVerfGE 65,1 = NJW 1984, 419).

Sicherlich bestand der besondere Verdienst des Bundesverfassungsgerichts darin, das Recht auf informationelle Selbstbestimmung und damit auf Datenschutz zum ersten Male im Sinne eines Grundrechts in den Mittelpunkt seiner Betrachtungen zu stellen. Wobei in diesem Zusammenhang auch das so genannte Quellensteuerurteil des Bundesverfassungsgerichts (BVerfGE 84, 239 = NJW 1991, 2129, 2132), in dem das Gericht endgültig alle Zweifel über den Grundrechtscharakter des Datenschutzes beseitigte, in Erinnerung gebracht werden muss.

Den Datenschutz hat das Bundesverfassungsgericht jedoch mit diesen beiden Entscheidungen keineswegs „erfunden“.

Bereits Ende der 60iger Jahre begann in Deutschland vor dem Hintergrund des immer weiter zunehmenden Vordringens der Datentechnik und Datenverarbeitung und bedingt durch die Entwicklung großer Rechenzentren die Diskussion um den Schutz der Privatsphäre unter den von der automatisierten Datenverarbeitung gesetzten Maßstäben.

Schon früh erkannte man, dass das schon Ende des 19. Jahrhunderts in den USA formulierte und im Jahre 1950 auch in die Europäische Menschenrechtskonvention eingebrachte und hierdurch geschützte Recht auf Privatsphäre argen Gefährdungen durch die übergroßen und letztlich unkalkulierbaren Möglichkeiten der Datenverarbeitung ausgesetzt war.

Die Diskussion der hierbei widerstreitenden Auffassungen und Interessen dieser ersten Jahre der Datenschutzüberlegungen fanden ihren Niederschlag in dem im Auftrag der Bundesregierung erstellten Gutachten zu den Grundfragen des Datenschutzes („Grundfragen des Datenschutzes“, Steinmüller, Lutterbeck, Mallmann, Harbort, Kolb und Schneider, Juli 1971, BT-Drs. VI/3826).

Schon vor Fertigstellung dieses Gutachtens wurde von einem deutschen Bundesland das weltweit erste Datenschutzgesetz erlassen.

Es war Hessen, das mit seinem Datenschutzgesetz vom 07.10.1970 (GVBl. I, S. 625) den ersten Meilenstein auf dem Wege der Datenschutzgesetzgebung setzte.

Nachdem im Jahre 1973 Schweden als erster Staat ein Datenschutzgesetz erließ, folgte im Jahre 1974 unser Nachbarland Rheinland-Pfalz (dort hatte es bemerkenswerterweise von dem ersten, von der damaligen CDU-Landtagsfraktion im Jahre 1971 eingebrachten, Gesetzesentwurf bis zur Verabschiedung des Landesdatenschutzgesetzes im Januar 1974 fast drei Jahre gebraucht).

Weitere Bundesländer folgten mit eigenen Gesetzen und im Jahre 1981 schloss der Stadtstaat Hamburg mit seinem Datenschutzgesetz die Gesetzesbemühungen der (alten) deutschen Bundesländer ab. Die neuen Bundesländer erließen nach ihrem Beitritt zur Bundesrepublik Deutschland in rascher Folge ihre Landesdatenschutzgesetze. Das Bundesdatenschutzgesetz datiert vom 28. Januar 1977 (BGBl. I, S. 201).

Wie reihte sich nun das Saarland in diese Entwicklung ein?

Nun, in seiner Sitzung am 17. Mai 1978 verabschiedete der Landtag des Saarlandes einstimmig das Saarländische Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Saarländisches Datenschutzgesetz – SDSG), das vom Ministerpräsidenten am 7. Juni 1978 ausgefertigt und am 28. Juni 1978 im Amtsblatt des Saarlandes (S. 581 ff.) veröffentlicht wurde. Seine wesentlichen Bestimmungen traten am 1. Juli 1978 in Kraft.

Die Landesregierung ernannte Dr. Gerhard Schneider durch Beschluss vom 3. Oktober 1978 mit Zustimmung des Landtages durch Beschluss vom 11. Oktober 1978 zum Landesbeauftragten für Datenschutz. Die Einführung in sein Amt erfolgte am 20. Oktober 1978.

Dr. Gerhard Schneider bekleidete dieses Amt bis zu seinem Ausscheiden in den Ruhestand im Frühjahr 1995.

Der Saarländische Landtag wählte ihn auf Vorschlag der Landesregierung jeweils in drei Amtsperioden. Dies geschah zudem einstimmig, was nicht nur seine unabhängige Stellung gegenüber der Exekutive stärkte, sondern für seine Persönlichkeit und die damit verbundene Amtsführung auf einem nicht a priori konfliktfreien Arbeitsgebiet sprach.

Wesentlich hilfreich war ihm hierbei, dass er bereits als zuständiger Referent maßgeblichen Anteil an der Vorbereitung und Umsetzung des Saarländischen Datenschutzgesetzes von 1978 hatte und damit über eine unbestrittene Fachkompetenz auf dem damals noch relativ neuen Gebiet des Datenschutzes verfügte.

Ihm gelang es, in der Pionierzeit des Datenschutzes „Pflöcke einzuschlagen“ und landesgesetzliche Grundlagen in den verschiedenen Rechtsgebieten mit zu schaffen. Herrn Dr. Schneider kommt nicht allein dadurch, dass er mit dem Auf- und Ausbau der Dienststelle des Landesbeauftragten für Datenschutz zu einer arbeitsfähigen und vor allem, trotz ihrer Kleinheit, in besonderem Maße leistungsfähigen – damals schon – Dienstleistungsbehörde Besonderes realisiert hat, sondern auch für seine Verdienste um die Fortentwicklung des Datenschutzes im Saarland eine herausgehobene Vorbildfunktion zu.

Als Nachfolger von Dr. Schneider wählte der Saarländische Landtag am 8. November 1995 Herrn Leitenden Ministerialrat Bernd Dannemann zum Landesbeauftragten für Datenschutz.

Herr Dannemann, der seine vielfältigen Tätigkeiten im Bereich verschiedener Ministerien und innerhalb der Staatskanzlei in dieses Amt einbringen konnte, schied mit Ablauf des Jahres 2001 aus dem aktiven Dienst des Landes aus. Auch er hat die Entwicklung des Datenschutzes im Saarland und darüber hinaus maßgeblich mit beeinflusst. Sein besonderes Verdienst dabei war es zu erkennen, dass sich aufgrund der rasanten technischen Entwicklung der Datenschutz von der eher grundsätzlichen Rechtsthematik zu den Problemen der technischen Umsetzung der bereits geltenden rechtlichen Regelungen hin entwickelt hat.

Vor allem aber gelang es ihm, dem Datenschutz dadurch mehr Akzeptanz und damit mehr Geltung zu verschaffen, dass er den Schwerpunkt von einer früher eher nachgängigen Kontrolltätigkeit hin zur präventiven Unterstützung und Beratung der Behörden und sonstigen Stellen verlagerte.

Doch zurück zum historischen Abriss des Datenschutzes im Saarland.

Bis zum Inkrafttreten des Saarländischen Datenschutzgesetzes galt vom 1. Januar 1978 bis zum 30. Juni 1978 in der öffentlichen Verwaltung des Saarlandes, soweit dieses Bundesrecht ausführte, das Bundesdatenschutzgesetz. Ausgenommen waren die Vorschriften über die Bundesverwaltung und über die Kontrolle des Datenschutzes. Keine gesetzliche Regelung für den Datenschutz bestand in dieser Zeit für die Ausführung des Landesrechts durch öffentliche Stellen.

Eine einheitliche Rechtsgrundlage für den Datenschutz in der öffentlichen Verwaltung gibt es damit erst seit dem Inkrafttreten des Saarländischen Datenschutzgesetzes.

Auf Grund des Gesetzes zur Änderung des Gesetzes über den Landtag des Saarlandes und des Saarländischen Besoldungsgesetzes vom 13. Juli 1978 (Amtsblatt des Saarlandes S. 697) bildete der Landtag zur Wahrnehmung seiner Rechte aus dem Saarländischen Datenschutzgesetz einen Ausschuss für Datenschutz.

Dieser wurde zunächst als Unterausschuss des (ständigen) Ausschusses für Inneres durch Beschluss des Innenausschusses vom 17.10.1978 gebildet. Die erste Sitzung des Unterausschusses für Datenschutz fand am 09.01.1979 unter dem Vorsitz des damaligen Abgeordneten und jetzigen Präsidenten des Landgerichts Günther Schwarz statt.

Am 02.04.1990 beschloss der Landtag, einen eigenen Ausschuss für Datenschutz zu bilden. Dieser wurde am 02.05.1990 eingerichtet und tagte unter dem Vorsitz des Abgeordneten Horst Edig am 03.09.1991 erstmals.

Seit dem ersten Inkrafttreten des Saarländischen Datenschutzgesetzes ist dieses mehrfach geändert worden. Die letzte grundlegende Änderung hat der Landtag am 22.08.2001 beschlossen (Gesetz Nr. 1477 vom 22.08.2001, Amtsblatt S. 2066).

Die überaus interessante Arbeit, die Entwicklung des Datenschutzes in seiner Gesamtheit während der letzten 25 Jahre anhand der Änderungen des Saarländischen Datenschutzgesetzes darzustellen, kann an dieser Stelle (leider) nicht geleistet werden.

Eine – zudem bedeutungsvolle – Änderung darf jedoch an dieser Stelle noch eine kurze Erwähnung finden:

Seit seiner Institutionalisierung im Jahre 1978 war der Landesbeauftragte für Datenschutz vom damaligen Innenministerium auch mit der Wahrnehmung der Aufgaben der Aufsichtsbehörde im nicht-öffentlichen Bereich betraut worden.

Als im Jahre 1993 das Datenschutzgesetz geändert und der Landesbeauftragte dem Landtag zugeordnet wurde, ist die Zusammenfassung der Datenschutzkontrolle für den privaten Bereich und die öffentlichen Stellen aufgegeben worden. (Auf Vor- und Nachteile dieser Zweiteilung der Kontrollkompetenz gehe ich noch unten unter Ziffer 3.1 näher ein.)

Überaus positiv war jedoch die Angliederung der Dienststelle des Landesbeauftragten für Datenschutz an den Landtag zu bewerten.

Sie führte letztlich zur Vermeidung jedweder Interessenkollision und stärkte die Unabhängigkeit des Landesbeauftragten.

Diese wiederum ist den Bürgerinnen und Bürgern dieses Landes Garant für das in Artikel 2 Satz 2 der Saarländischen Verfassung verbriefte Recht auf Datenschutz.

Diese Festschreibung des Datenschutzes in der Saarländischen Verfassung – ein schon sehr früh erwogenes Vorhaben (vgl. Zweiten Teilbericht der Enquetekommission für Verfassungsfragen gemäß Beschluss des Landtages vom 18. Februar 1976) – nahm der Landtag in der auslaufenden 8. Legislaturperiode vor.

Sie ist ebenfalls ein unbestreitbar wichtiger Meilenstein auf dem Wege der Verbesserung der rechtsstaatlichen Handhabung der Grundrechte, explizit des Grundrechtes auf Datenschutz und darf nicht deshalb unterschätzt werden, weil das Bundesverfassungsgericht die bestimmenden Grundsätze des Datenschutzes aus dem Grundrecht der Menschenwürde (Art. 1 Abs. 1 GG) und den persönlichen Freiheitsrechten (Art. 2 Abs. 1 GG) hergeleitet hat und deshalb mit der Änderung der Landesverfassung keine eigentliche Rangerhöhung verbunden sei. Letztere Auffassung verkennt den unschätzbar wichtigen Beitrag der Landesverfassungen, so auch der unsrigen, den diese hinsichtlich des Schutzes der Grundrechte zu leisten im Stande sind.

Auch aus diesem Grunde bedeuten 25 Jahre Datenschutz im Saarland ein Vierteljahrhundert Schutz des Persönlichkeitsrechts, des Menschenrechts auf Achtung der Privatsphäre und des Rechts, Herr über die eigenen ganz persönlichen Daten zu sein (Grundrecht auf informationelle Selbstbestimmung).

In den vergangenen 25 Jahren hat der Saarländische Gesetzgeber ständig seine Bereitschaft unter Beweis gestellt, den Respekt vor der informationellen Selbstbestimmung in einer Zeit der (fast) nicht mehr zu bremsenden Fortentwicklung der Informationsgesellschaft und ihrer technischen Möglichkeiten zu garantieren.

Man kann mit Fug und Recht behaupten, dass der Datenschutz sich in den letzten 25 Jahren im Lande etabliert hat. Er wird weitgehend von allen Beteiligten akzeptiert. Nicht als lästiges Übel, sondern, aus der Erkenntnis heraus, dass Datenschutz mit Grundrechtsschutz gleich zu setzen ist, als ebenso notwendig wie selbstverständlich. Im Zeitalter einer allgegenwärtigen, weltweiten Datenverarbeitung ist effektiver Datenschutz nicht nur für die betroffenen Bürgerinnen und Bürger von Nutzen, sondern letztlich auch für die verantwortlichen öffentlichen Stellen.

Dabei können – und dies soll, durchaus selbstkritisch, nicht verkannt werden - die Art und das Verständnis von der Erfüllung der Aufgaben eines Datenschutzbeauftragten sich sowohl in positiver aber auch in negativer Weise auf das eigentliche Ziel, Grundrechte zu schützen, auswirken.

Datenschutz sozusagen als Überzeugungstäter mit dem Ofenrohrblick eines Fundamentalisten betreiben zu wollen, ist deshalb genauso wenig angebracht, wie ein legerer Umgang im Sinne einer zudem falsch verstandenen Liberalität.

Es gilt vielmehr, die Balance zwischen der wirksamen Erfüllung staatlicher Aufgaben und dem individuellen Persönlichkeitsrecht des Einzelnen, das sich auch in dem Grundrecht auf informationelle Selbstbestimmung manifestiert, zu finden. Eine Wechselbeziehung, die der sorgfältigen Abwägung bedarf.

Dies führt dazu, dass die Tätigkeit eines Landesbeauftragten für Datenschutz oftmals weniger von spektakulären, weithin sichtbaren Erfolgen, als von, durch kleine aber beharrliche Schritte erreichte, stille Erfolge geprägt ist.

In Erkenntnis dieser Realitäten bin ich mir sicher, dass es auch weiterhin möglich sein wird, unseren saarländischen Bürgerinnen und Bürgern effektiven Datenschutz zu garantieren. Dass die Belange des Datenschutzes von den öffentlichen Stellen dieses Landes, bis hinauf zu den Obersten Landesbehörden, Ernst genommen und praktiziert werden, wird dabei auch künftig ebenso selbstverständlich sein, wie das bereits in der Vergangenheit gerne angenommene Angebot des Landesbeauftragten für Datenschutz an alle öffentlichen Stellen des Landes, im Sinne einer Dienstleistungsbehörde bereits im Vorfeld von Gesetzesvorhaben, beim Erlass von Verordnungen und Verwaltungsvorschriften sowie bei vielen anderen, aus einer breiten IT-Anwendung resultierenden Problemstellungen beratend zur Seite zu stehen.

Dies alles im Sinne der Verwirklichung des Grundrechtes auf informationelle Selbstbestimmung.

Der Ausspruch des ehemaligen englischen Premierministers William Ewart Gladstone (1808-1898)

„It is liberty alone which fits man for liberty“

(Allein die Freiheit befähigt den Menschen zur Freiheit)

kann dabei durchaus programmatisch für ein weiteres Vierteljahrhundert Datenschutz im Saarland sein.

1.2 Allgemeine Betrachtungen

Es gibt vieles, was, losgelöst von den Ereignissen im Saarland, im Laufe des Berichtszeitraumes besondere Aufmerksamkeit erregt hat und deshalb auch besondere Erwähnung an dieser Stelle verdienen würde.

Auf zwei Dinge möchte ich mich jedoch in meiner kurzen Darstellung beschränken: Die Ereignisse des 11. September 2001 und ihre Auswirkungen auf den Datenschutz einschließlich der Rasterfahndung sowie auf ein Urteil des Bundesgerichtshofs, das in einem gegen einen Kollegen gerichteten Strafverfahren erging und von grundsätzlicher Bedeutung für die Arbeit der Datenschutzbeauftragten des Bundes und der Länder ist.

1.3 Die Ereignisse des 11. September 2001 und ihre Auswirkungen auf den Datenschutz

Es steht – auch für die Datenschützer – zweifelsfrei fest, dass die Terroranschläge des 11. September 2001 uns in jeder Hinsicht mit Verbrechen konfrontiert haben, die in dieser Dimension bisher nicht für möglich gehalten worden sind.

Die Auswirkungen trafen nicht nur die USA, sondern die gesamte Welt. Sie ließen dabei die Verwundbarkeit gerade einer offenen, von demokratischen Strukturen geprägten Gesellschaft in sehr schmerzhafter Art und Weise spürbar werden. Für alle an der Prävention oder Repression beteiligten Stellen und Behörden eröffneten die Ereignisse in den USA eine völlig neue Dimension.

Auch für die durch die Geschehnisse besonders geforderten Datenschutzbeauftragten des Bundes und der Länder.

Dabei hat sich in gesteigertem Maße gezeigt, dass Terrorismusbekämpfung eine weltweite Herausforderung darstellt und damit nicht von nationaler Gesetzgebung allein, noch dazu wirkungsvoll, geleistet werden kann.

Folge des 11. September 2001 war eine überaus rege, teilweise mehr der Schnelligkeit und dem internationalen Druck huldigende als dem Gebot der Gründlichkeit folgende gesetzgeberische Tätigkeit im Bund – aber auch in den Ländern.

Sicherheitsgesetzgebung in der Bundesrepublik Deutschland existiert keinesfalls erst seit dem 11.09.2001. Zahlreiche Gesetze gegen Terrorismus, organisierte Kriminalität, Hooligans und auch Rechtsextremismus zeigen, dass insbesondere die als so genannte Schily-Sicherheitspakete („Otto-Katalog“) bekannt gewordene Terrorismusbekämpfungsgesetzgebung nur zum Teil direkte Antwort auf die Anschläge vom 11. September 2001 ist.

Darüber hinaus mussten viele der in den „Sicherheitspaketen“ enthaltenen Einzelmaßnahmen nicht neu erfunden werden.

Eine große Zahl der fast einhundert Einzelgesetze betreffenden Regelungen waren bereits im Zusammenhang mit den Diskussionen um die innere Sicherheit seit RAF-Zeiten entwickelt worden und lagerten sozusagen „abrufbereit“ in Referentenschubladen.

Das erste Sicherheitspaket umfasste zwei wesentliche Regelungen:

Einmal wurde nach den Querelen um den Kölner Kalifat-Staat das Religionsprivileg im Vereinsgesetz gestrichen (Erstes Gesetz zur Änderung des Vereinsgesetzes v. 04.12.2001, BGBl. I 2001, 3319). Diese Regelung entzieht gewaltbereiten Gruppen weitestgehend die Deckung, die sie dadurch genossen, dass sie nicht dem Vereinsgesetz unterlagen.

Zum anderen wurde mit der am 26.04.2002 vom Bundestag beschlossenen Fassung des Strafrechtsänderungsgesetzes - § 129 b StGB (34. StÄndG vom 22.08.2002, BGBl. I, 3390) die bisherige tatbestandliche Beschränkung (vgl. § 129 a StGB) auf kriminelle und/oder terroristische Vereinigungen mit einer räumlich-organisatorischen Inlandsverankerung aufgegeben und die Strafhoheit auf exterritorial organisierte terroristische Vereinigungen ausgedehnt.

Diese Regelung trägt der internationalen Vernetzung, dem weltweiten Aktionsradius und der zunehmenden Außensteuerung terroristischer Gruppierungen Rechnung und war ein erster Schritt zur Umsetzung der Rahmenbeschlüsse zur Terrorismusbekämpfung der EU (Rahmenbeschlüsse aus 2002). § 129 b StGB bezieht sich in erster Linie auf organisationsfördernde bzw. den terroristischen Zielen der Gruppierung dienende grenzübergreifende Aktivitäten im Rahmen einer (durch Sach- oder Handlungsbezug) begründeten Inlandsverknüpfung als Legitimation für eine Strafschutzausdehnung.

Dabei ist eine ins Grenzenlose ausufernde Strafausdehnung durch die vorausgesetzte Inlandsanknüpfung der begangenen Handlungen, also durch das vorausgesetzte Hineinwirken in inländische Schutzbelange ausgeschlossen.

Die Debatten im Bundestag und Bundesrat um den § 129 b brachten noch eine Vielzahl von in diesem Zusammenhang ungelösten Problemen mit sich (Reichweite des Tatbestandes des „Werbens“), die die Anrufung des Vermittlungsausschusses erforderlich machten. Der Vermittlungsausschuss bestätigte mit seinem Einigungsvorschlag vom 12.06.2002 den Beschluss des Bundestages. Mit der Zurückweisung des hiergegen am 21.06.2002 vom Bundesrat eingelegten Einspruchs (Art. 77 III GG) durch den Bundestag war zu rechnen. § 129 b StGB ist m.W.v. 30.08.2002 in Kraft.

Das sehr umfängliche zweite Sicherheitspaket ist als „Gesetz zur Bekämpfung des internationalen Terrorismus („Terrorismusbekämpfungsgesetz“) zum 11. Januar 2002 in Kraft getreten (Gesetz vom 09.01.2002, BGBl I. vom 11.01.2002, 361).

Es wurde in rekordverdächtigem Tempo am 14.12.2001 vom Bundestag und bereits sechs Tage später am 20.12.2001 vom Bundesrat verabschiedet.

Bezeichnend für die ungewöhnliche Eile war, dass am 01.01.2002 die Bundesregierung auf ihrer Homepage eine Pressemitteilung verbreitete, wonach das Terrorismusbekämpfungsgesetz am gleichen Tage in Kraft getreten sei, obwohl zu diesem Zeitpunkt der Bundespräsident noch prüfte, ob er das Gesetz ausfertigen kann. Dies tat er am 09.01.2002. In Kraft getreten ist das Gesetz – trotz gegenteiliger Regelung in seinem Art. 22 (der vom 01.01.2002 ausgeht) – erst am 11.01.2002.

Das Terrorismusbekämpfungsgesetz dient der Verbesserung der Aufklärungsmöglichkeiten und beinhaltet zusätzliche Kompetenzen für die Sicherheitsbehörden und einen verstärkten Datenaustausch zwischen diesen. Außerdem ermöglicht es nach bundes- und landesrechtlichen Vorgaben eine Rasterfahndung auch unter Einbeziehung von Sozialdaten zur Enttarnung so genannter Schläfer.

Das Terrorismusbekämpfungsgesetz änderte in 22 Artikeln folgende Gesetze: BundesverfassungsschutzG, MADG, BNDG, Artikel 10 G, Sicherheitsüberprüfungsgesetz, Bundesgrenzschutzgesetz, Passgesetz, Personalausweisgesetz, Vereinsgesetz, BKAG, Ausländergesetz, Asylverfahrensgesetz, Ausländerzentralregistergesetz (AZRG), Verordnung zur Durchführung des Ausländergesetzes, Ausländerdateienverordnung, AZRG-DurchführungsVerordnung, Bundeszentralregistergesetz, SGB X, Luftverkehrsgesetz, Luftverkehrszulässigkeitsüberprüfungsverordnung, Energiereduzierungsgesetz 1975, Elektrizitätsverteilungsverordnung, Gaskostenverteilungsverordnung.

Das Sicherheitspaket II erweitert vor allem die Rechte des Bundesamtes für Verfassungsschutz zur Informationsgewinnung. Mit dem Ziel, die Einholung von Informationen über Geldströme und Kontobewegungen von Organisationen und Personen, die extremistischer Bestrebungen oder sicherheitsgefährdender bzw. geheimdienstlicher Tätigkeiten verdächtigt werden, zu ermöglichen, wurde dem Bundesamt für Verfassungsschutz die Befugnis eingeräumt, Informationen über Konten und Kontoinhaber einzuholen.

Darüber hinaus wurden Befugnisse des BfV zur Informationsgewinnung gegenüber Postdienstleistern, Luftverkehrsunternehmen, Telekommunikations- und Teledienstanbietern vorgesehen.

Gleichfalls erweitert wurden die originären Ermittlungskompetenzen sowie die Möglichkeit der Informationsbeschaffung des BKA.

Dem BGS wurde die Möglichkeit eingeräumt, im Rahmen seiner erweiterten räumlichen und sachlichen Zuständigkeit Personen nicht nur anzuhalten und zu befragen, sondern auch die mitgeführten Ausweispapiere zu überprüfen.

Daneben ermöglicht es den Einsatz bewaffneter Flugbegleiter des BGS (sog. Sky-Marshals).

In das Ausländergesetz, das AsylVerfG und das AZRG wurden Regelungen aufgenommen, die die gesetzlichen Voraussetzungen für identitätssichernde Maßnahmen und einen behördlichen Informationsaustausch schaffen. Dies dient in erster Linie mit dazu, die Einreise terroristischer Straftäter nach Deutschland zu verhindern.

Im Sicherheitsüberprüfungsgesetz (SÜG) wurden nunmehr erstmals Vorschriften für Maßnahmen des vorbeugenden personellen Sabotageschutzes geschaffen. Personen, die in lebens- oder verteidigungswichtigen Einrichtungen tätig sind oder tätig werden sollen, werden nunmehr zuerst sicherheitsüberprüft.

Regelungen im Luftverkehrsgesetz schaffen die gesetzliche Grundlage für Zuverlässigkeitsüberprüfungen hinsichtlich des bei Flugplatz- und Luftfahrtunternehmen in sicherheitsrelevanten Bereichen beschäftigten Personals.

Im Passgesetz bzw. im Personalausweisgesetz wiederum wurde die Grundlage geschaffen, um Personen auf der Grundlage der Ausweisdokumente computerunterstützt zu identifizieren. Der Pass bzw. Personalausweis darf neben den bereits vorhandenen biometrischen Merkmalen weitere biometrische Merkmale von Fingern, Händen oder Gesicht des Dokumenteninhabers enthalten. Diese können auch in mit Sicherheitsverfahren verschlüsselter Form in das Personaldokument eingebracht werden.

Die Datenschutzbeauftragten des Bundes und der Länder haben unmittelbar nach den Ereignissen des 11. September 2001 den Kampf des demokratischen Rechtsstaates gegen Terrorismus und organisierte Kriminalität mit Nachdruck unterstützt. Sie waren dabei stets zu einem offenen und konstruktiven Dialog über notwendige Anpassungen an die neue Bedrohungslage bereit, haben aber von übereilten Maßnahmen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger einschränken, gewarnt (vgl. Entschließung Anlage 6).

Die Datenschutzbeauftragten haben dabei gefordert, dass neue Eingriffsbefugnisse nicht pauschal ausgerichtet, sondern zielgenau auf konkrete Gefährdungssituationen im terroristischen Bereich zugeschnitten und von vornherein befristet werden.

Letztlich auch durch den entschiedenen Einsatz der Datenschutzbeauftragten fanden beim Erlass des Terrorismusbekämpfungsgesetzes wesentliche Forderungen des Datenschutzes Berücksichtigung.

So ist die Geltung zahlreicher Änderungen auf fünf Jahre beschränkt worden. Zudem sind sie vor Ablauf dieser Frist zu evaluieren.

Darüber hinaus wurden die Auskunftsrechte des Bundesamtes für Verfassungsschutz – und entsprechend diejenigen der Landesämter für Verfassungsschutz – strengen Verfahrensvorschriften unterworfen und die Einrichtung einer bundesweiten Zentraldatei für biometrische Merkmale ausdrücklich gesetzlich ausgeschlossen.

Auch konnte erreicht werden, dass im Rahmen einer Rasterfahndung Gesundheitsdaten von den Sozialbehörden nicht an die Polizei übermittelt werden dürfen.

Als weiterer Erfolg ist zu werten, dass dem Bundeskriminalamt entgegen ursprünglicher Planungen nicht die Befugnis eingeräumt wurde, Vorermittlungen ohne Anfangsverdacht im Sinne der Strafprozessordnung durchzuführen.

1.4 Die Rasterfahndung

Einige der Täter und Hintermänner der terroristischen Anschläge am 11.09.2001 hatten sich, wie entsprechende polizeiliche Ermittlungen sehr rasch ergaben, vor der Tat völlig unauffällig in Deutschland aufgehalten und sich von hier aus langfristig auf die Anschläge vorbereitet.

Nach dem Jargon des „Spionagegeschäfts“ werden Personen, die ausgewählt, ausgebildet und im gegnerischen Lager unauffällig platziert werden, um erst bei einer bestimmten Konstellation subversiv oder nachrichtendienstlich tätig zu werden, „Schläfer“ benannt.

Was lag näher, als die mit Bezug zu Deutschland enttarnten Attentäter ebenfalls als „Schläfer“ zu bezeichnen und dem aufgekommenen Verdacht nachzugehen, dass weitere „Schläfer“ in Deutschland unerkannt leben.

Um diese Personen zu enttarnen, wurde von den Polizeibehörden eine bundesweite Rasterfahndung durchgeführt.

Im Rahmen der Rasterfahndung wurden bei öffentlichen und privaten Stellen personenbezogene Daten erhoben. So z.B. bei Hochschulen, Meldeämtern, Ausländerbehörden, aber auch bei Industrie- und Handelskammern.

Der Rasterfahndung lagen weit gefasste Suchkriterien zu Grunde, wobei vom Persönlichkeitsprofil der Attentäter ausgegangen wurde: Männlich, 18-40 Jahre alt, islamistische Religionszugehörigkeit, Ausländer mit legalem Aufenthaltsstatus, Student oder ehemaliger Student aus Ländern des nahen und fernen Ostens, insbesondere aber aus sog. „Schurkenstaaten“ (z.B. Afghanistan). Auch Deutsche, die in einem solchen Land geboren sind, unterfielen dem Raster. Bei letzteren sind Angaben über Inhaber von Lizenzen für Gefahrguttransporte verlangt worden. Auch das Tätigsein in einem Atomkraftwerk, einem Chemiewerk, das Innehaben einer Fluglizenz oder eines Waffenscheins waren Suchkriterien, mit denen gerastert wurde.

Das Täterprofil des unauffälligen, unbescholtenen Mannes stellte im Polizeibereich ein völliges Novum dar. Im Grunde suchte man die Stecknadel im Heuhaufen. Besser gesagt: Man versuchte das Unmögliche.

Generalbundesanwalt Kay Nehm hat in seinem Versuch einer Schwachstellenanalyse der Bewältigung der Ereignisse um den 11.09.2001 die Figur des „Schläfers“ als eine „zur Exkulpation der Sicherheitsbehörden erfundene“ bezeichnet und ihr vor dem Hintergrund des bekannt gewordenen Verhaltens der Attentäter und ihres Umfeldes einen bitteren Beigeschmack attestiert (Nehm, NJW 2002, 2665 (2670).

Hinweisen wollte er damit auf die Tatsache, dass die Attentäter des 11. September 2001 und ihre Helfer keinesfalls von der Kategorie „Schläfer“ umfasst werden konnten. Er wollte aber auch – fast schon provokant – auf die Frage hinweisen, ob die sich aus unserer Vergangenheit begründeten Restriktionen 50 Jahre nach Gründung der BRD vor dem Hintergrund aktueller Gefährdung als unzeitgemäß und hinderlich erwiesen haben. Dies brachte er dadurch zum Ausdruck, dass er eine Neubesinnung im Vorfeld der Vorsorge von terroristischen Gefahren forderte. Er war der Ansicht, dass, wenn man die Lebensläufe der Terroristen Revue passieren lässt, immer wieder auffällt, wie sehr vermeintliche religiöse Toleranz und Fremdenfreundlichkeit sowie großzügige Duldungs- und Einbürgerungspraxis zu einer islamistisch-fundamentalistischen Subkultur beigetragen hätten (derselbe aaO, S. 2671).

Geradezu elektrisierend auf Datenschützer aber wirkt allerdings die Frage des Generalbundesanwalts, ob nicht der administrative Datenschutz mit sorgfältiger Missbrauchskontrolle ein besserer Weg sei als ein formelles Streben nach gesetzlicher Datenschutzperfektion (derselbe aaO).

Diese Fragestellung impliziert das grundsätzliche Infragestellen gerade des Grundrechts auf Datenschutz.

Immerhin konzediert der Generalbundesanwalt noch die Notwendigkeit eines stringenten Datenschutzes im nachrichtendienstlichen Bereich.

Es wundert bei solchen Grundaussagen daher auch nicht, dass die Datenerhebungen im Zuge der Rasterfahndung nicht klaglos hingenommen wurden. Weder von den von ihr Betroffenen, noch von den angerufenen Gerichten. Auch nicht von den Datenschützern. Letztere sprachen sich nicht grundsätzlich gegen die Möglichkeit einer Rasterfahndung aus, wohl aber energisch gegen Bestrebungen, die in den Polizeigesetzen der Länder enthaltenen Eingriffsschwellen für die Durchführung von Rasterfahndungen herabzusetzen. Dies besonders deshalb, weil von der Rasterfahndung – wie sich nachträglich herausstellte – zu fast einhundert Prozent nur unbescholtene Bürger betroffen waren.

Eine Bewertung der Wirksamkeit von bestimmten polizeilichen Befugnissen und Maßnahmen – so auch der Rasterfahndung – ist grundsätzlich schwierig und mit vielen Unwägbarkeiten behaftet. Solange kein klarer Erfolg einzelner Maßnahmen nachgewiesen werden kann – und dieser Beweis konnte bislang nicht erbracht werden – sind Zweifel an ihrer Wirksamkeit nie auszuschließen. Andererseits kann der als Erfolg zu wertende Effekt solcher Maßnahmen vielfältig sein. Schon die denkbare Störung der Infrastruktur einer kriminellen Vereinigung durch die von einer Rasterfahndung ausgehende Erhöhung des Fahndungsdrucks beispielsweise kann als ein solcher Erfolg gewertet werden, ohne dass dieser Effekt nachgewiesen oder gar quantifiziert werden könnte. Auch aus Sicht der Datenschützer ist damit hier wie in vielen vergleichbaren Bereichen (etwa den polizeilichen Eingriffen in die Telekommunikation, dem Einsatz verdeckter Ermittler etc.) durch den Gesetzgeber eine Güterabwägung vorzunehmen. Schwerwiegende Gefährdungen rechtsstaatlicher Güter können auch den Einsatz von in ihrem Erfolg eher ungewissen Eingriffsbefugnissen rechtfertigen, wenn andere staatliche Abwehrmaßnahmen nicht vorhanden oder noch schwächer wirksam sind, wenn der rechtsstaatliche Kernbereich nicht tangiert wird und wenn auch die Belastung der betroffenen Individuen noch als verhältnismäßig angesehen werden kann. Im Ergebnis vertritt auch die bisherige Rechtsprechung bei der verfassungsrechtlichen Prüfung der polizeilichen Rasterfahndung diese Auffassung.

Insgesamt gesehen ist festzustellen, dass sich der Staat seit dem 11. September 2001 innerhalb des Spannungsbogens von Freiheit und Sicherheit vom Brennpunkt der Freiheit zum Brennpunkt der Sicherheit bewegt hat. Zu dieser Bewertung muss man auch bei objektiver Betrachtung der gesetzgeberischen Aktivitäten nach dem 11. September 2001 leider kommen.

Bleibt zu hoffen, dass es in der Folge nicht auch zu einem nachhaltig grundlegenden Wandel der Gesellschaft insgesamt kommen wird.

In den „Krieg gegen den Terrorismus“ ist die Zivilgesellschaft, gegen die sich eine Vielzahl der Überwachungsmaßnahmen richtet, zwangsläufig – und nicht nur informationstechnisch – mit einbezogen.

Ohne den Fortbestand der Grundrechte, insbesondere des Grundrechts auf informationelle Selbstbestimmung führt aber der Weg in eine Gesellschaft, in der die Bürger immer weniger Autonomie haben werden.

Es ist Aufgabe auch und gerade der Datenschutzbeauftragten, einer solchen Entwicklung entschieden entgegen zu treten.

Die Grundlage für eine offene demokratische Gesellschaft ist nicht der Gedanke „weniger Freiheit, mehr Sicherheit“, sondern die Maxime „Freiheit durch Sicherheit“ (Karl Popper, Die offene Gesellschaft und ihre Feinde, Bd. I, 6. Auflage, 1980).

1.5 Neues zur Rechtsstellung der Datenschutzbeauftragten

Eine Entscheidung des 5. Strafsenats des Bundesgerichtshofes verdient es, an dieser Stelle erwähnt zu werden (Urteil vom 9.12.2002 – 5 StR 276/02, NJW 2003, 979 ff.).

Diese Entscheidung brachte das gegen meinen sächsischen Kollegen gerichtete Strafverfahren wegen mehrfacher Verletzung des Dienstgeheimnisses zu einem Ende. Der Bundesgerichtshof verwarf die Revision der Staatsanwaltschaft und bestätigte damit die Entscheidung des Landgerichts Dresden, das den Sächsischen Datenschutzbeauftragten zuvor vom Vorwurf der Verletzung des Dienstgeheimnisses in drei Fällen freigesprochen hatte. Den Urteilen lag, in aller Kürze geschildert, der folgende Sachverhalt zugrunde:

Nach mehrfachen Hinweisen darauf, dass der Sächsische Staatsminister der Justiz in einem staatsanwaltschaftlichen Ermittlungsverfahren in unlauterer Weise auf die Staatsanwaltschaft eingewirkt haben könnte, prüfte der Sächsische Datenschutzbeauftragte die Angelegenheit und sprach letztendlich eine (förmliche) datenschutzrechtliche Beanstandung aus. Zuvor hatte er bereits mehrfach versucht, auch unter Einschaltung des Chefs der Sächsischen Staatskanzlei, den Minister zu einer anderen Verhaltensweise sowie zur Änderung von Verwaltungsvorschriften, die die Berichtspflichten der Staatsanwaltschaft betrafen, zu bewegen.

Aufgrund erheblichen Drucks seitens der Öffentlichkeit (sprich: insbesondere der Presse) verlas der Datenschutzbeauftragte in zwei Pressekonferenzen sowohl die vom Justizminister stammenden und in der entsprechenden Akte angebrachten Verfügungen als auch seine gesamte datenschutzrechtliche Beanstandung im Wortlaut. Das Beanstandungsschreiben übermittelte er auch an seinen Petenten.

Unabhängig davon, dass der betroffene Minister wenig später zurücktrat, mündete das gegen den Sächsischen Datenschutzbeauftragten eingeleitete staatsanwaltschaftliche Ermittlungsverfahren in ein Strafverfahren vor der 4. Großen Strafkammer des Landgerichts Dresden, die den angeklagten Datenschutzbeauftragten von allen drei Tatvorwürfen freisprach.

Diese Entscheidung wurde vom 5. Strafsenat des Bundesgerichtshofes mit im Wesentlichen folgenden, für die Arbeit aller Datenschutzbeauftragten der Länder und des Bundes ebenso wichtigen wie richtungweisenden Begründungen bestätigt:

Der Angeklagte habe zwar Geheimnisse gemäß § 353 b Abs. 1 StGB offenbart. Auch rechtswidriges Verhalten Dritter könne eine geheimhaltungsbedürftige Tatsache sein. Doch sei hier eine Gefährdung wichtiger öffentlicher Interessen im Sinne dieser Vorschrift zu verneinen.

Selbst eine mittelbare Gefährdung, die nach der Rechtssprechung des Bundesgerichtshofes grundsätzlich im Einzelfall ausreichen kann und die in einem Verlust des Vertrauens der Öffentlichkeit in die Integrität des Datenschutzbeauftragten durch den Geheimnisbruch bestehen könne, scheide aus.

Ein Amtsträger, der wie z.B. ein Datenschutzbeauftragter, zur Kontrolle der Gesetzestreue eines anderen Amtsträgers berufen ist, könne wichtige öffentliche Interessen nicht durch die Offenbarung eines Gesetzesverstoßes gefährden, wenn er auch die Öffentlichkeit als Verbündeten zur Erwirkung gesetzmäßigen Verhaltens gewinnen will. Damit verfolge, so der Bundesgerichtshof, der Datenschutzbeauftragte selbst ein wichtiges öffentliches Interesse, was einen Verlust des Vertrauens hinsichtlich der Integrität des Datenschutzbeauftragten in der Öffentlichkeit ausschließt. Ein Verlust des Vertrauens der Öffentlichkeit in die Integrität des kontrollierten Amtsträgers hingegen kann nach Auffassung des Bundesgerichtshofes keine wichtigen öffentlichen Interessen begründen.

Auch die Unterrichtung des Petenten über den festgestellten Datenschutzverstoß und damit zusammenhängend die Übersendung der datenschutzrechtlichen Beanstandung (im vollen Wortlaut) an ihn führt nach der überzeugenden Auffassung des Bundesgerichtshofes nicht zu einer Strafbarkeit wegen Offenbarung von Dienstgeheimnissen.

Ausdrücklich betont hat der Bundesgerichtshof darüber hinaus die Anzeigebefugnis des Datenschutzbeauftragten.

2 Technisch-organisatorischer Datenschutz

2.1 Telearbeit bei der Finanzverwaltung

Schon 1997 hatte das damalige Ministerium für Wirtschaft und Finanzen ein Projekt „Telearbeit Saar“ gestartet, das sich in Zusammenarbeit mit saarländischen Projektpartnern zum Ziel gesetzt hatte, die Telearbeit in einem Pilotszenarium zu erproben und dabei auch Anwendungsmöglichkeiten in der öffentlichen Verwaltung zu untersuchen.

2001 trat dann das Ministerium für Finanzen und Bundesangelegenheiten mit dem konkreten Projekt an mich heran, Telearbeitsplätze in der Finanzverwaltung, insbesondere bei den Finanzämtern einzurichten und dazu die Rahmenbedingungen zu erörtern.

Die Verarbeitung personenbezogener Daten, die hier dem Steuergeheimnis unterliegen, bedarf eines erhöhten Schutzes, der nach meiner Ansicht nicht im Rahmen von Telearbeit gewährleistet werden kann. Auch bei optimaler Ausgestaltung des Arbeitsplatzes ist die Finanzverwaltung nicht in der Lage, die tatsächliche Ausführung ihrer Anweisungen zu überwachen. Selbst regelmäßige Kontrollen hätten nicht den gleichen Effekt wie die in den Behördenräumen wirksam ausgeübte ständige Dienstaufsicht. Vor allem aber ergibt sich ein Kontrolldefizit daraus, dass ein unbeschränktes Zugangsrecht zur Privatwohnung – im Gegensatz zu Diensträumen – schon wegen der Grundrechtsgarantie des Artikels 13 Grundgesetz nicht besteht. Selbst bei einem vertraglich vereinbarten Zugangs- und Kontrollrecht zum häuslichen Arbeitsplatz, das im übrigen auch auf den Landesbeauftragten für Datenschutz ausgeweitet werden müsste, ließe sich im Falle einer Einrede des Bediensteten oder eines Mitbewohners der Wohnung die Kontrolle nicht ohne weiteres durchsetzen. Aus diesem Grunde habe ich darum gebeten, von der Einrichtung von Telearbeitsplätzen Abstand zu nehmen, wenn sensible personenbezogene Daten zu verarbeiten sind.

Nachdem die Finanzverwaltung die Zielsetzung weiter verfolgte und auf mein Betreiben hin signalisierte, sich auf drei Einzelprojekte (Betriebsprüfung, Rechtsbehelfsstelle, Programmierung bei der ZDV-Saar) zu beschränken, habe ich meine Bedenken für die Zeit der Erprobung zurückgestellt. Hinsichtlich der zu treffenden technischen und organisatorischen Maßnahmen habe ich einen hohen Standard gefordert, der der Sensibilität der Daten angemessen sein sollte.

Die Projektarbeitsgruppe legte dann im Rahmen ihres umfangreichen Berichts eine „Vorläufige Rahmendienstvereinbarung über die Erprobung der Heim-/Telearbeit“, eine „Vereinbarung über die Errichtung eines außerbehördlichen Heim-/Telearbeitsplatzes“ und eine „Erklärung über das Zutrittsrecht zum Heimarbeitsplatz“ zur Abstimmung vor. Die Ausgestaltung der technischen und organisatorischen Maßnahmen erfolgte unter Berücksichtigung des Schutzstufenkonzepts der IT-Sicherheitsrichtlinie des Saarlandes in Abstimmung mit meiner Dienststelle. Insbesondere soll die ISDN-Verbindung mit Hilfe der vom Bundesamt für die Sicherheit in der Informationstechnik BSI entwickelten SINA-Architektur gesichert werden, die über eine Chipkarte den Zugang zu den Komponenten schützt und über eine VPN-Anbindung (virtual privat network) mit IPSEC-Absicherung die Daten zwischen Arbeitsplatz-PC und Dienstellen-Server verschlüsselt überträgt.

Die Datensicherheit bei der Aufbewahrung von Unterlagen in Aktenform darf bei alledem ebenfalls nicht außer Acht gelassen werden.

2.2 Verschlüsselung im Landesdatennetz

Auf Grund eines 1988 vom Ministerium für Wirtschaft und Finanzen in Auftrag gegebenen „Gutachtens über das Telekommunikationsnetz der saarländischen Landesverwaltung“ beschäftigte sich die dazu gebildete Arbeitsgruppe auch mit einem möglichen Outsourcing des Landesdatennetzes an private Dienstleister. Das Gutachten empfahl die Zusammenlegung der bisher 5 landesweiten Kommunikationsnetze und zeigte auch die Alternative auf, alle TK-Anlagen der Behörden nur noch virtuell dezentral darzustellen und sie zentral zusammen zu fassen und dort durch einen privaten Dienstleister administrieren zu lassen. Nachdem ein potentieller Anbieter als einfache Anbindung an sein Netz auch eine Funkstrecke ins Gespräch gebracht hatte, untersuchte ich die Risiken einer solchen Lösung und wies auf die damit verbundenen Risiken hin, worauf die Arbeitsgruppe von dieser Lösung Abstand nahm. Bei der als Alternative aufgezeigten zentralen Administration durch Private zeigte ich die damit verbundenen Risiken auf und verwies auf die Orientierungshilfe „Wartung und Fernwartung“ der Datenschutzbeauftragten des Bundes und der Länder, in der geeignete Maßnahmen zur Beherrschung der Risiken dargestellt sind.

Schon im Rahmen der 1998 in Angriff genommenen Privatisierung der Datenverarbeitung des Landes hatte ich eine generelle Verschlüsselung der Datenübertragung im Landesdatennetz als Basis-Dienstleistung gefordert. Bei diesem Projekt erhob ich die Forderung erneut, wobei es gelang, die Landesverwaltung von der Notwendigkeit einer Absicherung der Übertragung zwischen den Verwaltungsnetzknoten zu überzeugen. Damit sollte sichergestellt werden, dass ein beliebiger Netzbetreiber auf beliebigen Leitungen die Datenströme der Verwaltung übertragen kann, ohne die Inhalte der oft sensiblen und auch personenbezogenen Daten zur Kenntnis nehmen zu können. Je nach Sensibilität der Daten kann dann bei Bedarf noch eine Ende-zu-Ende-Verschlüsselung ergänzend genutzt werden.

Inzwischen ist eine entsprechende Ausschreibung auf Basis der auch im Informationsverbund Berlin-Bonn und beim TESTA-Netz der öffentlichen Verwaltung eingesetzten SINA-Verschlüsselung erfolgt und es ist damit zu rechnen, dass der durch Verschlüsselung zusätzlich abgesicherte Betrieb des Landesdatennetzes 2003 realisiert wird.

2.3 Funk-Vernetzung im Bereich der öffentlichen Verwaltung

Das Rechenzentrum der Universität des Saarlandes hatte sich bei einem Projekt „Wireless LAN“ des Bundesministeriums für Bildung und Forschung beworben, bei dem pro Bundesland bis zu zwei Demonstrationsvorhaben zur Einführung einer drahtlosen Netzwerkinfrastruktur zum Einsatz in der Lehre gefördert werden sollten und auch einen entsprechenden Zuschlag erhalten. Das Projekt sollte offiziell im März 2001 in Betrieb gehen. Mit dieser sehr interessanten neuen Technik kann eine aufwändige Verkabelung in Gebäuden entfallen und damit den Gegebenheiten vor allem auch bei historischer Bausubstanz oder nur vorübergehend genutzten Gebäuden oder auch bei Veranstaltungen Rechnung getragen werden. Über das Funk-Netz ist dann ein Zugriff auf das Rechnernetz der Universität und darüber z. B. auch zum Internet mit Hilfe von Laptops an beliebiger Stelle in der Universität möglich. Die Reichweite solcher Funkverbindungen beträgt im Freien bis zu 400 m bis zum nächsten Access-Point, ist aber abhängig von eventuellen Abschirmungen (z.B. Betonarmierungen), wodurch die Reichweite auf bis zu 30 m in Gebäuden zurückgehen kann.

Das Hauptproblem bei Funkvernetzung aus Sicht des Datenschutzes ist, dass solche Funk-LANs prinzipiell offen sind für „Eindringlinge“ und „Zuhörer“, die die freie Funk-Übertragung unerkannt missbräuchlich nutzen können. Als Schutz dagegen können folgende Techniken genutzt werden:

- Wireless Domain Names (SSID = Service Set ID) und Codes als Identifikation
- Filter für festgelegte Protokolle im Netz oder festgelegte Clients (z. B. MAC-Adresse der Netzwerkkarte)
- NAT = Netzwork Adress Translation mit IP-Masquerading zum Schutz der Internas gegen Kenntnisnahme von außen
- Access-Control-List ACL mit MAC-Adressen, wobei entweder die Adressen gelistet sind, die zulässig sind, oder die Adressen, die unzulässig sind oder eine Kombination davon; dabei sind die ersten 24 Bits fest eingestellte Firmenadressen (OUI = Organisationally Unique Identifier), die vom IEEE verbindlich vergeben werden (siehe standards.ieee.org/reganth/oui/)
- Basis-Verschlüsselung mit WEP 40- oder WEP 64-Verfahren; dieses Verfahren arbeitet mit 64 Bit RC4-Algorithmus, wobei 24 Bits als so genannter „Initial Vector“ vom Algorithmus selbst errechnet werden und der Anwender nur 40 Bit frei wählen kann; diese Verschlüsselung wird nicht als sehr sicher angesehen

zusätzliche IPSEC-Verschlüsselung der Übertragung.

Während die Uni Rostock als erster Projektpartner bei der Funk-Übertragung generell mit einer WEP-Verschlüsselung arbeitet und damit eine Basis-Verschlüsselung vorausgesetzt ist, wollte die Uni Saarbrücken darauf verzichten und lediglich „auf Wunsch“ des Funk-LAN-Teilnehmers eine IPSEC-Verschlüsselung ermöglichen. Die Nutzung einer solchen Verschlüsselung setzt also zusätzliche Aktivitäten der Nutzer voraus, die vermutlich aus Bequemlichkeit unterlassen werden dürften.

In der Regel sollten bei der Universität des Saarlandes Anwender erst zugelassen werden, wenn ihre PC-Card mit ihrer MAC-Adresse bei der Anwenderberatung registriert wurde. Für Gäste sollte allerdings auch ein unregistrierter Zugang zugelassen werden, bei dem der Zugriff nur auf bestimmte Netzzugänge beschränkt werden sollte, womit allerdings auch weitere Zugangsmöglichkeiten eröffnet werden, die missbraucht werden könnten. Da das Funk-LAN als Zugang für alle Anwendungen im Uni-Netz genutzt werden sollte, ist die Art der darüber übertragenen Daten nicht eingegrenzt. Es können unter Anderem personenbezogene Daten unterschiedlicher Sensibilität übertragen werden (z. B. auch Benutzerkennungen und Passwörter). Insofern halte ich eine zwangsweise vorhandene Basisverschlüsselung (so wie bei der Uni Rostock) für dringend erforderlich. Bei höherer Sensibilität der personenbezogenen Daten kann dann eine individuelle Ende-zu-Ende-Verschlüsselung (z. B. PGP, Sphinx) zusätzlich für angemessene Sicherheit sorgen.

In einem letzten Gespräch hat das Rechenzentrum zugesagt, keine unregistrierten Zugänge zuzulassen, eine WEP-Verschlüsselung einzurichten und eine ergänzende IPSEC-Verschlüsselung zu implementieren. Die von mir geforderte Risikoanalyse und das Sicherheitskonzept zur Funkvernetzung liegen bisher noch nicht vor.

Im Rahmen der Landesinititative „INTEL - Lehren für die Zukunft“ wurde auch ein Gymnasium mit funkvernetzten Laptops ausgestattet, die im Unterricht nicht aber in der Schulverwaltung verwendet werden sollen. Da es nicht ausgeschlossen werden kann, dass dabei auch personenbezogene Daten über die Funkstrecke übertragen werden können, habe ich auch für diesen Einsatzfall auf die Problematik hingewiesen und eine Risikoanalyse und ein Sicherheitskonzept gefordert, was auch vorgelegt wurde. Das Ergebnis wird dem Ministerium für Bildung, Kultur und Wissenschaft zur Unterrichtung der Schulen und dem Landesinstitut für Pädagogik und Medien zur Projektbetreuung und Fortbildung der Lehrer zur Verfügung gestellt.

2.4 „Kabinett-Online“ und Verschlüsselung

Mit Unterstützung der Stabsstelle für Innovation, Forschung und Technologie bei der Staatskanzlei wurde das bundesweit einmalige Projekt „Kabinett Online“ realisiert. In einer ersten Ausbaustufe wurde ein Intranet eingerichtet, auf das nur die Kabinettreferate, die Minister und Staatssekretäre und der Ministerpräsident mit ihren Laptops zugreifen konnten. Auf einem zentralen Server werden Sitzungsvorlagen und –protokolle zum Zugriff bzw. Abruf vorgehalten, die Gesetzesentwürfe, Verordnungen, Vorlagen, Berichte, Personalangelegenheiten und Parlamentarische Anfragen enthalten.

Auf Grund der teilweise hohen Sensibilität der Unterlagen und der dabei genutzten personenbezogenen Daten wurde auf meinen Vorschlag hin eine angemessene Verschlüsselung zur Absicherung der Übertragung und der lokalen Speicherung auf den Laptops erreicht.

2.5 Einheitliche eMail-Kommunikation in der saarländischen Landesverwaltung

In der Landesverwaltung steigt der Anteil der dienstlichen Kommunikation über eMail immer mehr an. Bedingt durch die historische Entwicklung kommen in den Behörden unterschiedliche Mail-Systeme zum Einsatz, durch die Probleme bei der Formatumwandlung entstehen können und übergreifende Groupware-Funktionalitäten wie z. B. Terminkalender, Aufgabenverwaltung oder Raumbelegung nicht nutzbar sind.

Aus diesen Gründen hatte sich eine Arbeitsgruppe darauf verständigt, als Client-Software generell das MS-Produkt „Outlook“ einzuführen und für die Groupware-Funktionen auf einen Verbund dezentraler Exchange-Server zu setzen. In einer ersten Ausbauphase sollte ein Ressort-übergreifender Querriegel für die Führungsebenen der Ressorts realisiert werden. In weiteren Schritten sollten die Ressorts eigene Exchange-Server aufbauen und neben dem Mailing auch Groupware-Funktionalitäten anbieten. Zur Erleichterung der Nutzung sollte ein zentrales LDAP-Adressverzeichnis dienen. Der Umfang der dort präsentierten Daten und die Zugriffsmöglichkeit durch die saarländischen Behörden wurden mit mir einvernehmlich abgestimmt. Zu beachten ist auch, dass die Landesregierung in einer gemeinsamen Geschäftsordnung (GGO) die private Mitnutzung von eMail untersagt hat, so dass die aus einer privaten Nutzung folgende, besondere Behandlung des Mail-Verkehrs wegen des damit verbundenen Fernmeldegeheimnisses hier nicht berücksichtigt werden musste.

Ergänzend zu den technischen Tests habe ich von der Arbeitsgruppe eine Risikoanalyse und ein Sicherheitskonzept gefordert. Mein Hauptaugenmerk liegt dabei auf einer einfach zu handhabenden Verschlüsselung beim Mail-Versand, gegebenenfalls ergänzt durch eine elektronische Signatur sowie auf der Absicherung der weitreichenden Zugriffsrechte der Administratoren. Dabei soll das von der Bundesverwaltung favorisierte Verfahren „Sphinx“ und das schon in der Landesverwaltung eingesetzte Verfahren „PGP“, das auch weltweit und im privaten Bereich Standard ist, auf seine Integrationsmöglichkeit hin betrachtet werden. Wichtig ist auch ein Online-Virenschutz auf den beteiligten Servern und Arbeitsplatzrechnern, wobei die Problematik verschlüsselter Mails bzw. Anlagen berücksichtigt werden muss. Die Arbeitsgruppe hat zur Abstimmung einen ersten Entwurf vorgelegt, der noch verfeinert werden soll. Eine Testumgebung für den Querriegel ist fertig gestellt und muss noch begutachtet werden.

2.6 Schulung nach dem Saarländischen Datenschutzgesetz

Ende 2001 trat die Neufassung des SDSG in Kraft, die insbesondere einen behördlichen Datenschutzbeauftragten als Option und eine generelle Vorabkontrolle bei neuen Verfahren einführte und die bisherige Dateibeschreibung durch eine Verfahrensbeschreibung ersetzte.

Wegen des zu erwartenden dringenden Bedarfs in der öffentlichen Verwaltung und des Fehlens geeigneter Schulungsangebote entschloss ich mich, in Kooperation mit dem Ministerium für Inneres und Sport und dem Ministerium für Frauen, Arbeit, Gesundheit und Soziales eine entsprechende Schulung anzubieten. Obwohl bei diesem Schulungstermin 70 Teilnehmerplätze vorhanden waren, war die Nachfrage so enorm, dass ich eine zweite Veranstaltung anbieten musste. Aber auch hier war noch eine so hohe Anmeldezahl festzustellen, dass ich nach dauerhaften Lösungen suchte. Inzwischen ist es gelungen, in Zusammenarbeit mit dem Schulungsbereich des TÜV-Saarland eine Veranstaltungsreihe zu initiieren, die diesen Bedarf abdecken soll und offen ist für weitere Fortbildungen im gesamten Themenbereich des Datenschutzes und der Datensicherheit.

Als Hilfe für die Behörden habe ich eine Arbeitsfassung des neuen SDSG entworfen, eine Merkblatt für die nach § 6 erforderliche Unterrichtung erstellt und ein elektronisches Formular für die Verfahrensbeschreibung entwickelt und alle diese Materialien auf meiner Internet-Seite bereitgestellt. Ergänzend dazu habe ich auf der Basis der neuen Regelungen Vorschläge für eine Überarbeitung der IT-Sicherheitsrichtlinie des Saarlandes und der IT-Projektrichtlinien unterbreitet, die jetzt 2003 in Kraft gesetzt werden sollen.

2.7 Begleitung des Internet-Angebots der Landesverwaltung

Anfang des Jahres 2000 begann die Landesverwaltung mit der Konzipierung einer integrierten Internet-/Intranet-Lösung. Ziel sollte sein, unter dem Stichwort „Kunden- und Service-Orientierung“ ein Portal für aktive Bürger und alle Mitarbeiter zur Verfügung zu stellen, bei dem auch aktuelle Informationen abrufbar sein sollten. Die Internet-Lösung basierte auf einer gemeinsamen Plattform mit weitgehend identischem Design, gleicher Struktur und ähnlichen Inhalten, an der sich die Ressorts mit ihren nachgeordneten Dienststellen orientieren sollten.

In enger Abstimmung mit der federführenden Staatskanzlei gelang es, auch die datenschutzrechtlichen Aspekte zur Geltung zu bringen, wobei auch hier die Kooperationsbereitschaft der Staatskanzlei durchaus vorbildlich war. Dabei wurde unter anderem die Zulässigkeit der präsentierten personenbezogenen Daten überprüft und auch über mögliche Navigationspunkte und Präsentationstechniken diskutiert. Das Design und die Präsentation wurden um einige kritische Elemente reduziert und um eine Datenschutz- und Haftungsinformation ergänzt. Es konnte auch erreicht werden, dass in der Präsentation von Organigrammen und Geschäftsverteilungsplänen lediglich die Führungsebene namentlich genannt wird und ansonsten eine funktionale Beschreibung der Aufgaben und der Kontaktmöglichkeiten, z. B. auch eine funktionale eMail-Adresse, benutzt wurde.

Die mit der Staatskanzlei abgestimmte Präsentation diente den nachfolgenden Angeboten der Ressorts und der zugehörigen Dienststellen als Muster, so dass bei einer Prüfung im Rahmen der Freigabe in der Regel eine sofortige positive Stellungnahme aus datenschutzrechtlicher Sicht möglich war. Allerdings musste bei der Umsetzung in einzelnen Fällen zuerst einmal die Funktionalität von Suchmaschinen an Hand der Namenseingabe des Gesprächspartners konkret vorgeführt werden, um bei den Betroffenen ein entsprechendes Risikobewusstsein zu erzeugen, wonach dann doch die Präsentation von Mitarbeiterdaten auf den unbedingt notwendigen Umfang reduziert werden konnte.

Parallel dazu beschäftigte sich eine Arbeitsgruppe mit der Einrichtung eines verwaltungsinternen Intranets. Neben ressort-spezifischen Informationen für die eigenen Mitarbeiter sollten auch verwaltungsintern alle Informationen bereitgestellt werden, die im normalen Dienstgang benötigt werden. Dazu gehören aus datenschutzrechtlicher Sicht z. B. auch Telefonverzeichnisse und Geschäftsverteilungspläne. Nach sorgfältiger Abwägung aller Aspekte hatte ich mich damit einverstanden erklärt, dass diese Informationen in einem LDAP-Verzeichnisdienst nicht nur in den Ressorts und ihren nachgeordneten Dienststellen abrufbar sein sollten, sondern auch in anderen Dienststellen der öffentlichen Verwaltung wie z. B. den Gemeinden und Kreisen. Lediglich bei einem eventuellen Anschluss der Verzeichnisse an landes- oder bundesübergreifende Verwaltungsnetzwerke sollte eine Beschränkung der Präsentationen unter besonderer Abwägung der Erforderlichkeit erfolgen. Zur Zeit wird überlegt, die Intranet-Verzeichnisse auch zur Präsentation der öffentlichen Schlüssel für eine Verschlüsselung oder elektronische Unterschrift zu nutzen. Die Pflege seiner Daten kann jeder Mitarbeiter selbst durchführen, was die Administration der Verzeichnisse wesentlich erleichtert.

Vor der Freigabe der Internet-/Intranet-Verfahren wurde mir Gelegenheit zu umfangreichen Tests gegeben, wobei Erkenntnisse aus dem einen Bereich auch im anderen umgesetzt wurden. Die Erstellung der Konzepte, der Struktur und der Inhalte der Präsentationen erfolgte erfreulicherweise in enger Abstimmung mit meiner Dienststelle, so dass auch bei der zukünftigen Weiterentwicklung davon ausgegangen werden kann, dass die datenschutzrechtlichen Belange vollständig beachtet werden.

2.8 Prüfung der Internet-Angebote der Gemeinden und Kreise, eGovernment

Die Präsentation der Gemeinden und Kreise in einem eigenen Internet-Angebot als Dienstleistung für den Bürger ist mit wenigen Ausnahmen inzwischen selbstverständlich. Nicht immer selbstverständlich war hingegen – im Unterschied zur Landesverwaltung – die Einsicht, auch datenschutzrechtliche Belange in hinreichendem Maße zu berücksichtigen. Bei der Gestaltung dieser Angebote wurden und werden oft die Vorschläge und Ideen privater Dienstleister, Bürger-Arbeitskreise oder innovativer Mitarbeiter umgesetzt, die sich eher an der im Werbebereich üblichen Präsentationsformen orientieren und die damit verbundenen Risiken sowie rechtliche, insbesondere datenschutzrechtliche Belange vernachlässigen.

Um mir einen Überblick zu verschaffen, habe ich alle erreichbaren Internet-Angebote der Gemeinden und Kreise überprüft und ausgewertet. Dabei musste ich feststellen, dass es oft üblich ist, die Internet-Seiten mit Hilfe von potentiell gefährlichen aktiven Inhalten attraktiver und mit Hilfe von Cookies auf den Benutzerrechnern einfacher zu gestalten. Im Sinne des neuen Leitbildes „Modern und Bürgernah“ werden zum Teil umfangreiche Mitarbeiterdaten bis hin zu ihren Bildern und privaten Hobbys präsentiert, obwohl nach § 4 SDSG eine Datenvermeidung und Datensparsamkeit vorgeschrieben ist. Oft wird dazu auch die Einwilligung der Betroffenen eingeholt, die aber nicht zu einer Beschränkung der Veröffentlichungen führt, da die Bediensteten es in der Regel als Ehre ansehen, im Internet-Angebot der Stellen persönlich genannt oder sogar mit Bild dargestellt zu werden und oft auch noch glauben, dass dies unkritisch sei, da man sie ja nur finden würde, wenn man gezielt auf das Angebot zugreift. Die Auswerte- und Verknüpfungsmöglichkeiten von Suchmaschinen sind in der Regel nicht bekannt und es herrscht auch die irrige Meinung vor, dass solche Suchmaschinen-Bezüge gelöscht würden, wenn das bezogene Angebot modifiziert oder gelöscht wurde. Außerdem setzen sich Bedienstete, die eine Veröffentlichung ihrer Daten aus guten Gründen ablehnen würden, dem Vorwurf aus, nicht modern und bürgernah zu sein und nicht dem neuen Leitbild der Dienststelle zu entsprechen, was alle anderen für selbstverständlich halten. Insofern ist ihre Zustimmung oft auch gar nicht mehr freiwillig. Oft ist auch die persönliche Darstellung von Bediensteten nicht hilfreich, da diese wegen Urlaub, Schulung, Dienstreise und Krankheit gar nicht erreichbar sind. Bei eMail-Adressen werden oft der Vorname und der Name als Standard für die Gestaltung benutzt (z. B. fritz.mueller@gemeinde.de). Für die Kontaktaufnahme mit einer Stelle (z. B. Hundesteuer) ist es allerdings ausreichend und datenschutzfreundlich, eine funktionale Adresse zu veröffentlichen (z. B. steueramt@gemeinde.de). Dies schließt nicht aus, dass dann in der Individualkommunikation zwischen Bürger und Bedienstetem eine persönliche eMail-Adresse benutzt wird; sie sollte nur nicht durch eine Internet-Präsentation zusätzliche Risiken für den Bediensteten mit sich bringen. Aus diesen Gründen sollte eine Veröffentlichung von Bedienstetendaten im Sinne einer Datenvermeidung und Datensparsamkeit möglichst vermieden werden; dazu gehören insbesondere auch Bilder und Hobbys bzw. private Aktivitäten von Bediensteten. Bei Behördenwegweisern reicht zum Ansprechen der zuständigen Stellen eine funktionale Beschreibung aus, wozu auch die Darstellung von funktionsbezogenen eMail-Adressen gehört.

Als Hilfe für die betroffenen Behörden habe ich mich mit allen dafür Verantwortlichen unterhalten und mit ihnen die kritischen Aspekte des jeweiligen Angebotes diskutiert. Zusätzlich habe ich eine Checkliste für die Internet-Angebote erstellt und diese Stellen aufgefordert, damit das Angebot noch einmal zu überprüfen. Die Checkliste soll auch bei neuen Angeboten eine Hilfestellung bieten. Ergänzend dazu habe ich Materialien für geeignete Regelungen im Bereich Internet/eMail gesammelt und auf meinen Internet-Seiten bereitgestellt.

Wenn Internet-Angebote auf externen Servern von Dienstleistern bereitgestellt werden, werden dabei auch personenbezogene Daten der Zugreifer verarbeitet. Es handelt sich damit um eine Auftragsdatenverarbeitung, die gemäß § 5 SDSG zu regeln ist; oft allerdings werden Billigangebote von Webhostern genutzt, bei denen die Behörde nur die Wahl hat, die vorgelegten AGB´s zu akzeptieren, oder auf die Dienstleistung zu verzichten. Als Hilfe habe ich einen Muster-Vertrag für diese Auftragsdatenverarbeitung entwickelt und bereitgestellt.

Die Entwicklung im Internet-Bereich geht weiter und wird jetzt auch in Richtung „eGovernment“, d. h. einer elektronischen Kommunikation der Behörden mit dem Bürger, den Unternehmen und untereinander fortentwickelt. Die Datenschutzbeauftragten des Bundes und der Länder haben dazu eine Handreichung „Datenschutzgerechtes eGovernment“ entwickelt, die auch aus meinem Internet-Angebot abrufbar ist.

Darüber hinaus hat mir der Saarländische Städte- und Gemeindetag ermöglicht, meine datenschutzrechtlichen Vorstellungen im Zusammenhang mit einer Fachtagung zum Thema eGovernment einem breiten Personenkreis näher zu bringen. Ich halte gerade auch diese Form der Kooperation für einen guten Ansatz zur Lösung von Problemen.

Auf Initiative der Staatskanzlei und des Ministeriums für Wirtschaft arbeitet die Landesverwaltung inzwischen an einer Portal-Lösung für eGovernment. In die Konzeptentwicklung bin ich einbezogen und werde sie aus datenschutzrechtlicher Sicht begleiten.

In der Zukunft werde ich erneut eine Sichtung der Internet-Angebote vornehmen und dabei die Umsetzung der bisherigen Anforderungen überprüfen. In diesem Zusammenhang strebte ich auch eine enge Kooperation mit dem Saarländischen Städte- und Gemeindetag und dem Landkreistag an, um datenschutzgerechte Lösungen zur Umsetzung zu bringen. Zumindest bezüglich des Saarländischen Städte- und Gemeindetages ist es mir – wie oben dargestellt – zwischenzeitlich gelungen, die Zusammenarbeit auf ein gutes Fundament zu stellen. Ich bin mir sicher, dass mir dies auch mit Blick auf den Landkreistag gelingen wird.

2.9 Online-Wahlverfahren bei der Jugendgemeinderatswahl einer Gemeinde

Aus einer Presseinformation musste ich entnehmen, dass eine Gemeinde beabsichtigte, die Wahl des Jugendgemeinderats im Rahmen einer Online-Wahl über das Internet durchzuführen und durch die Nutzung des neuen Mediums für Jugendliche attraktiver zu gestalten. Insgesamt sollten dabei 1.700 Jugendliche und Erwachsene zwischen 14 und 21 Jahren angesprochen werden. Dass eine Beteiligung meiner Dienststelle vor der Freigabe des Verfahrens gesetzlich vorgeschrieben war, hatte die Gemeinde völlig übersehen.

Eine schnelle Überprüfung des schon fertig entwickelten und kurz vor dem Echteinsatz befindlichen Verfahrens zeigte, dass die benötigte Rechtsgrundlage höchst zweifelhaft war (der Bürgermeister hielt den Beschluss des Gemeinderates dazu für ausreichend) und das Verfahren selbst vor allem nicht den Anforderungen einer Wahl nach Vertraulichkeit und Sicherheit und auch nicht der von der Gemeinde selbst erlassenen Wahlordnung für die Wahl zum Jugendgemeinderat entsprach, in der eigentlich Papiergebundene Wahlscheine vorgesehen waren. Die vorgeschriebene Kontrolle der Stimmergebnisse durch einen Wahlvorstand bestand bei dem neuen Online-Verfahren lediglich aus einer Mitteilung der in der Datenbank enthaltenen Stimmergebnisse durch die Programmiererin. Die Software arbeitete mit potentiell gefährlichen aktiven Inhalten und Cookies auf den Nutzerrechnern. Arbeitsdateien des Online-Verfahrens auf dem Gemeindesever waren von außen lesbar und Stimmabgaben prinzipiell verfälschbar. Die Kandidaten waren mit ihren Daten und Bildern ohne schriftliche Zustimmung nach außen präsentiert worden. Die Programmiererin und Betreuerin des Online-Wahlverfahrens war nicht auf die korrekte Diensterfüllung nach dem Verpflichtungsgesetz und den Datenschutz verpflichtet worden. Das Verfahren und die einlaufenden Daten konnten von der Programmiererin auch während der Wahl von außen eingesehen und geändert werden.

Trotz dringender Hinweise des LfD gab der Bürgermeister das unvollkommene Verfahren zur Anwendung frei. Es gelang allerdings, noch zu Beginn des Verfahrensanlaufs in Abstimmung mit der Gemeinde das Verfahren weitgehend sicher zu machen und die genannten Mängel zu beseitigen. Die Probleme und datenschutzrechtlichen Anforderungen stellte ich dann in einer Presseerklärung heraus, damit andere Gemeinden eventuell beabsichtigte ähnliche Projekte zuvor mit mir abstimmen. Wie zu erfahren war, hat auch das Online-Wahlverfahren keine höhere Wahlbeteiligung erbracht. Die betroffene Gemeinde will trotzdem die nächste Wahl erneut online durchführen. Eine rechtzeitige Beteiligung meiner Dienststelle ist diesmal erfolgt. Entsprechende weitere Abstimmungsgespräche mit der Gemeinde sind im Gange.

2.10 Curriculum „Intel-Lehren für die Zukunft“ und Merkblatt „Schulen ans Netz - mit Sicherheit“

Aus einer Pressemitteilung der Landesregierung hatte ich entnommen, dass beim Landesinstitut für Pädagogik und Medien (LPM) ein Trainingszentrum in Betrieb genommen wurde, das von den Firmen INTEL und FUJITSU-SIEMENS mit Hard- und Software ausgestattet worden war. Das Land wollte die Fortbildung der Lehrer unter dem Arbeitstitel „INTEL-Lehren für die Zukunft“ finanziell fördern, wobei als Grundlage der Fortbildung ein umfangreiches, kostenloses Curriculum dienen sollte, womit die Lehrer „die neuen Medien und den Computer effektiv in ihren Unterricht integrieren“ sollten und besonderer Wert auf die Nutzung und die Präsentation mit Hilfe des Internet gelegt wurde.

Wie ich schon in meinem letzten Tätigkeitsbericht darlegte (18. TB S. 85), hat eine stichprobenartige Überprüfung der Internet-Nutzung an Schulen ergeben, dass dort die Anwendung der Technik im Vordergrund steht und rechtliche, vor allem aber datenschutzrechtliche Anforderungen nicht bekannt waren bzw. beachtet wurden. Insofern erhoffte ich mir aus dem nun zur Fortbildung benutzten Curriculum eine entscheidende Verbesserung der Situation dahingehend, dass ein Ausbildungsabschnitt sich auch mit den rechtlichen bzw. datenschutzrechtlichen Aspekten der Internet-Nutzung befassen würde. Doch weit gefehlt: außer einem kurzen Abriss zum Urheberrecht waren keine einschlägigen Informationen zum Thema ausgewählt worden.

Auf der Grundlage bereits ausgearbeiteter Materialien der Datenschutzbeauftragten entwickelte ich das Merkblatt „Schulen ans Netz – mit Sicherheit“, mit dem die fehlenden datenschutzrechtlichen Aspekte in die Curriculum-Ausbildung einfließen konnten. Das Merkblatt stellte ich dem LPM zur Verfügung und bat das Ministerium für Bildung, Kultur und Wissenschaft um Information aller Schulen, was nunmehr auf den Weg gebracht werden konnte. Es bleibt nur zu hoffen, dass fortgebildete Lehrer das entsprechende Wissen dann allmählich in ihren Schulen verbreiten oder in anderen Projekten (z. B. D21 siehe TZ 2.19) das entsprechende Know-How auf anderem Wege vermittelt wird. Die Broschüre wurde auch den anderen Datenschutzbeauftragten zur Verfügung gestellt, die sie teilweise an ihre Bildungsministerien weiter gaben, um damit auch die dort laufende Ausbildung zu ergänzen. Der bayerische Landesdatenschutzbeauftragte z.B. bemüht sich um eine entsprechende Überarbeitung des Curriculum in der nächsten Auflage. Das Merkblatt ist auch in meinem Internet-Angebot enthalten. Inzwischen hat auch ein Schul-Verlag das Merkblatt in seine Materialien-Sammlung übernommen, was – ohne unbescheiden zu sein – für Qualität, Praktikabilität und damit Akzeptanz meiner Handreichung spricht.

2.11 Sicherheit für den Internet-Arbeitsplatz

Die Nutzung des Internet am Arbeitsplatz nimmt immer mehr zu und dürfte in Zukunft die Regel sein, da nur so aktuelle Informationen wie z. B. auch die aktuellen Gesetzestexte für Jedermann zugreifbar sind. Da ich im Rahmen von Prüfungen in Schulen und Behörden feststellen musste, dass bei den Mitarbeitern nur ein geringe Kenntnisse über die damit verbundenen Risiken am Arbeitsplatz vorhanden waren und insbesondere auch wenig bekannt war, wie man mit einfachen Mitteln auch bei den Standard-Betriebssystemen, der Office-Software und den Internet-Browsern eine gewisse Sicherheit herstellen kann, habe ich ein Merkblatt „Der sichere Internet-Arbeitsplatz“ entwickelt, in dem die Risiken und entsprechende Gegenmaßnahmen beschrieben sind. Auch dieses Merkblatt wurde inzwischen von einem Schul-Verlag in seine Materialsammlung integriert und ist auch aus unserem Internet-Angebot abrufbar.

2.12 Gemeinsame Geschäftsordnung der Landesregierung

Die Landesregierung hatte eine Arbeitsgruppe mit der Erstellung einer „Gemeinsamen Geschäftsordnung (GGO) für die Obersten Landesbehörden“ beauftragt. Damit soll unter anderem ein bisheriger Organisationserlass entbehrlich und Verfahrensweisen bei der elektronischen Post geregelt werden.

Dankenswerterweise wurde ich von Anfang an in die Arbeit der Arbeitsgruppe einbezogen. An verschiedenen Stellen konnte ich datenschutzrechtliche Aspekte in die Vorlage einbringen. So wurde z. B. die Bestellung eines behördlichen Datenschutzbeauftragten verbindlich vorgeschrieben, eine geeignete Telefax-Regelung gefunden, die die bisher eigenständigen Telefax-Dienstanweisungen entbehrlich machte und in Anlage 2 die Nutzung von eMail auch unter datenschutzrechtlichen Gesichtspunkten einheitlich geregelt (siehe auch: TZ 2.5 Einheitliche eMail-Kommunikation in der saarländischen Landesverwaltung).

2.13 IT-Dienstanweisungen bei Gemeinden und Kreisen

Wie schon in meinem Tätigkeitsbericht für 1995 dargestellt, habe ich damals in Zusammenarbeit mit ausgewählten Behörden Muster-Dienstanweisungen erstellt und diese dann an alle in Frage kommenden Dienststellen mit der Bitte versandt, daraus angepasste Dienstanweisungen für den eigenen Bereich zu erstellen. Fast alle Behörden haben die gesetzlich vorgeschriebene Aufgabe ohne größere Probleme bewältigt.

Nur wenige Behörden versuchten zunächst, sich der Anforderung durch Einschaltung der zuständigen Kreisverwaltung oder sogar des Ministeriums für Inneres und Sport und mit Verweis auf fehlende personelle Ressourcen zu entziehen. Nachdem das Ministerium die Forderung des LfD unterstützte, bemühten sich weitere Gemeinden um eine Lösung. Bemerkenswerterweise „ruderten" besonders diejenigen als erste zurück, die vorher die „Speerspitze" des Widerstandes bildeten. Lange Zeit stand die Vorlage bzw. Inkraftsetzung einer Dienstanweisung leider noch bei einem Landkreis und zwei seiner Gemeinden aus, obwohl Hilfen angeboten wurden und in verschiedenen Besprechungen die Notwendigkeit vermittelt werden konnte und auch entsprechende Zusagen gemacht wurden. Durch persönliche Intervention bei der Bürgermeisterdienstbesprechung des entsprechenden Landkreises gelang es mir, dass zwischenzeitlich die beiden Gemeinden die IT-Dienstanweisungen erlassen haben. Die des Kreises wurde als Entwurf zur Abstimmung vorgelegt.

2.14 Musterhafte IT-Dienstanweisung des Rechnungshofes

Im Zuge einer Überarbeitung seiner Dienstanweisung unternahm der Rechnungshof die Anstrengung, eine Anweisung „aus einem Guss" zu erstellen und dabei die bisherige Telefax-Dienstanweisung zu integrieren und die neuen Anforderungen aus der Neufassung des Saarländischen Datenschutzgesetzes und einer eMail- und Internet-Nutzung mit zu regeln. Das Ergebnis ist gelungen und kann von anderen Behörden als Muster für ihre Überarbeitung herangezogen werden.

2.15 IT-Sicherheitskonzept für die Arbeitsgerichtsbarkeit

Das Ministerium für Frauen, Arbeit, Gesundheit und Soziales beabsichtigte die Gerichte für Arbeitssachen (Landesarbeitsgericht Saarbrücken, Arbeitsgerichte Saarbrücken, Saarlouis und Neunkirchen) mit einem modernen, integrierten Datenverarbeitungssystem auszustatten. Basierend auf den Erfahrungen mit der Erstellung eines musterhaften IT-Sicherheitskonzepts für das eigene Haus ging eine Arbeitsgruppe daran, auch für den Einsatz bei der Arbeitsgerichtsbarkeit ein angepasstes IT-Sicherheitskonzept zu erstellen. Auch hier kam die IT-Sicherheitsrichtlinie des Saarlandes in Verbindung mit dem IT-Grundschutzhandbuch des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) zur Anwendung. Das dazu eingerichtete IT-Sicherheitsmanagement entwickelte ein modellhaftes und datenschutzgerechtes Konzept, das auch die Besonderheiten der Software EUREKA-Fach berücksichtigte, die schon in einem Länderverbund von Niedersachsen, Hessen, Sachsen-Anhalt, Brandenburg, Schleswig-Holstein und Rheinland-Pfalz eingesetzt wurde. Dabei wurde auch ein Richterarbeitsplatz mit einem Spracherkennungssystem als Hilfe bei der Textbearbeitung getestet.

2.16 Neues Verfahren beim Landesamt für Verfassungsschutz

Verschiedene Prüfungen in der Vergangenheit führten zu der Erkenntnis, dass das beim Landesamt für Verfassungsschutz eingesetzte Verfahren zur Verwaltung der Datenbestände der Abteilungen in Teilbereichen nicht vollständig den datenschutzrechtlichen Anforderungen entsprach. Da sich auch herausstellte, dass das Programm Schwierigkeiten mit der Umstellung auf das Jahr 2000 hatte, wurde eine Neuprogrammierung in Auftrag gegeben, nachdem am Markt keine entsprechende Standard-Software angeboten wurde und auch kein Verfahren der Verfassungsschutzämter der anderen Bundesländer ohne großen finanziellen Aufwand übernommen werden konnte. Erfreulicherweise wurden das Konzept des neuen Verfahrens und dann auch das Verfahren selbst in allen wichtigen Entwicklungsschritten mit mir abgestimmt.

2.17 Datenschutzprobleme beim Ministerium für Bildung, Kultur und Wissenschaft

In der Vergangenheit gab es mehrere datenschutzrechtliche Aspekte, die vom Ministerium zögerlich bzw. gar nicht behandelt wurden.

So hatte ich schon in meinem 17. Tätigkeitsbericht im Zusammenhang mit der IT-Dienstanweisung des Ministeriums auf die fehlende Beteiligung meiner Dienststelle vor der Inkraftsetzung hingewiesen. Mit Schreiben vom 1.12.98 kündigte das Ministerium dann eine Zusammenfassung der unterschiedlichen und teilweise inkonsistenten Werke an. Mit der Neufassung des Saarländischen Datenschutzgesetzes und der Gemeinsamen Geschäftsordnung der Landesregierung (GGO) ist schon im letzten Jahr ein Ergänzungsbedarf entstanden.

Darüber hinaus musste ich feststellen, dass entgegen der GGO im Ministerium auch das private eMailen geduldet worden war, obwohl ich Hinweise gegeben hatte, dies GGO-gemäß zu regeln und für eine angemessene Absicherung des eMail-Verkehrs – auch mit den Schulen – zu sorgen.

Während es in Abstimmung mit der federführenden Staatskanzlei gelungen ist, in den Internet-Angeboten der Ressorts die Präsentation der personenbezogenen Daten der Bediensteten auf die Leitungsebene zu beschränken, durchbrach das MBKW diese Grenzen durch die Präsentation aller Mitarbeiter in einem nachgeordneten Bildungsserver.

Aus der Vergangenheit noch offen war auch die weitere Behandlung der aus der datenschutzrechtlichen Prüfung an ausgewählten Schulen verschiedener Schultypen Ende 2000 gewonnenen Erkenntnisse, bei der der dringende Bedarf der Schulen nach datenschutzrechtlicher Unterstützung, insbesondere auch bei den Internet-Angeboten und der Schulverwaltungssoftware, deutlich wurde. Zur Fortbildung der Lehrer habe ich ein Merkblatt „Schulen ans Netz – mit Sicherheit“, dessen Inhalte durch das Ministerium auch den nicht fortbildungswilligen Lehrern vermittelt werden sollten. Bei dieser Gelegenheit sollte auch die Umsetzung der Muster-IT-Dienstanweisung für Schulen und die Fragen nach datenschutzgerechter Standardsoftware für die Schulverwaltung behandelt werden.

In mehreren Schreiben hatte ich auf die veraltete, noch aus dem Jahre 1986 stammende „Verordnung über die Erhebung, Verarbeitung und sonstige Nutzung personenbezogener Daten in den Schulen“ hingewiesen. Auch stand noch eine dringende Regelung der Verarbeitung von Schülerdaten auf privaten Rechnern der Lehrer aus, nachdem das bisherige absolute Verbot der in den Schulen und bei den Lehrern praktizierten Verfahrensweise, insbesondere bei der Erstellung von Zeugnissen, nicht Rechnung trägt. Wie verschiedene Beispiele in anderen Bundesländern zeigen, könnten aber dafür datenschutzgerechte Regelungen gefunden werden, was ich durch Übergabe einer Lösung angeregt habe.

In der Vergangenheit wurde ich mehrfach in die Beurteilung unterschiedlicher Software zur Schulverwaltung eingebunden. Meinem Vorschlag, sich möglichst auf wenige, einheitliche Produkte für die verschiedenen Schulformen zu einigen, kam das Ministerium 1999 durch Auswahl des Verfahrens Magellan für den Sekundarbereich entgegen, das ich dann ebenfalls aus datenschutzrechtlicher Sicht bewertete. Durch eine einheitliche Verfahrensanwendung in den Schulen könnte nicht nur die Schulung und Betreuung vereinfacht, sondern auch die Datenübertragung zwischen Schulen und Ministerium standardisiert und gesichert und die Übernahme der statistischen Daten wesentlich erleichtert werden. Bisher ist die generelle Einführung im Sekundarbereich noch nicht erfolgt. Für den Grundschulbereich besteht jetzt auch noch die Gefahr, dass die Auswahl des dort eingesetzten Verfahrens den jeweiligen Schulträgern überlassen wird und dann unterschiedliche Produkte zum Einsatz kommen, wodurch die durch Standardisierung erreichbaren Vorteile für die Verfahrensbetreuung und die Datennutzung durch die Schulen und das Ministerium entfallen dürften und ein mehrfacher, datenschutzrechtlicher Bewertungsbedarf erzeugt wird.

Zur Betreuung der Schulen beginnt das Ministerium ein eigenes Service-Zentrum einzurichten. Da bei dieser Betreuung auch datenschutzrechtliche Aspekte eine große Rolle spielen dürften, wäre eine Zusammenarbeit mit den dortigen Mitarbeitern sinnvoll. Außerdem gibt es verschiedene Projekte wie z. B. „Saar-Lernnetz“, „Funk-Lan“, „Bildungsinititative Networking“, „Expertengruppe Pädagogisch-didaktische Konzepte“, die sicher auch einer datenschutzgerechten Begleitung bedürfen.

Nachdem zu diesen genannten Problemen entscheidende Lösungen des Ministeriums ausstanden, habe ich der Hausspitze in einem Grundsatzpapier die offenen Punkte dargestellt. Erfreulicherweise hat sich der Staatssekretär des Ministeriums für Bildung, Kultur und Wissenschaft persönlich darum gekümmert und die Arbeiten in Gang gebracht. Eine Überarbeitung der Dienstanweisungen wurde unter Berücksichtigung der musterhaften Dienstanweisung des Rechnungshofes in Angriff genommen. Das private eMailen wurde GGO-gemäß per Amtsverfügung untersagt. Die Präsentation der Mitarbeiterdaten auf dem Bildungsserver war schon datenschutzgerecht bereinigt worden; man hatte nur versäumt, den LfD davon in Kenntnis zu setzen. Die Umsetzung der Erkenntnisse der datenschutzrechtlichen Prüfung ist in Arbeit. Die genannte Verordnung wird überarbeitet, wobei auch die Verarbeitung von Schülerdaten durch Lehrer in deren häuslichen Bereich berücksichtigt werden soll. In Verbindung mit der Entscheidung der Landkreise zur Schulverwaltungssoftware im Sekundarbereich soll auch versucht werden, eine Aufsplittung der dazu verwendeten Software im Primarbereich zu vermeiden und die Anforderungen des Ministeriums für Schulstatistiken zu integrieren. Außerdem hat das Ministerium zugesagt, bei allen Projekten mit datenschutzrechtlichem Bezug den LfD künftig rechtzeitig zu beteiligen.

Mit der Hausspitze des MBKW wurde damit mehr als nur der Grundstein für eine mustergültige Zusammenarbeit gelegt.

2.18 Projekt „Saarland 21“ und Datenschutz

Unter dem Arbeitstitel „Saarland 21“ plante die Landesregierung ein umfangreiches Projekt „für den mündigen Bürger“, der sich über ein entsprechendes Internet-Angebot informieren und die Politik mitgestalten können soll. Leitprojekte firmierten dabei unter den Aspekten „Füreinander da sein“, „Initiative übernehmen“, „Courage zeigen“ und „In Schwung bleiben“. In die „Content-Planung“ wurde ich von Anfang an einbezogen. Dabei wurde nicht nur der Umfang der Präsentation bzw. Verarbeitung personenbezogener Daten mit mir besprochen, sondern auch die Nutzung von Gästebüchern, Foren und Chats datenschutzrechtlich geregelt und eine Datenschutzvereinbarung „Online-Privacy-Policy“ nach meinen Wünschen integriert.

2.19 Runder Tisch D21 Saarland

Unter dem Arbeitstitel „Runder Tisch D21 Saarland“ will die Landesregierung das Thema „Neue Medien im Unterricht“ in einem Feldversuch in zwei Landkreisen modellhaft erproben, wobei das Saarland eine Projektfinanzierung aus der Bundes-Initiative D21 zur Medienausstattung an allgemeinbildenden Schulen anstrebt. Das Ministerium lädt mich zu den Sitzungen der Arbeitsgruppe ein, die auch wissenschaftlich begleitet wird. Ich werde mich an der Unterarbeitsgruppe „Datenschutz und Datensicherheit“ beteiligen und dabei auch meine bisherigen Prüfergebnisse und Materialen für den Datenschutz in Schulen synergetisch einbringen.

2.20 ALIKA-Web und Sicherheit

Die Katasterverwaltung wollte mit Hilfe eines Web-basierten Abrufverfahrens für das Liegenschaftsbuch ALB ein flexibles und kostengünstiges Verfahren für die verschiedenen zugelassenen Nutzergruppen wie z. B. die öffentlich bestellten Vermessungsingenieure (ÖbVI), das Landesamt für Umweltschutz und das Landesamt für Straßenwesen realisieren. In enger Abstimmung mit meiner Dienststelle wurde das Verfahren konzipiert und schließlich, nachdem anfänglich eine SSL-Verschlüsselung vorgesehen war, ein VPN-Verschlüsselungsverfahren als Zugriffs- und Transportsicherung realisiert. Die Authentifizierung der zugriffsberechtigten Personen erfolgt über eine individuelle Benutzerkennung und ein Passwort. Die Einsatzreife des Verfahrens konnte dann bei einem ÖbVI modellhaft vorgeführt und dann das Verfahren freigegeben werden.

3 Übergreifende Themen

3.1 Saarländisches Datenschutzgesetz

Die Umsetzung der EG-Datenschutzrichtlinie in das Saarländische Datenschutzgesetz (Amtsbl. 2001, 2066) hat noch während der Amtszeit meines Vorgängers stattgefunden. Dieser hatte schon sehr frühzeitig dem Innenressort Vorschläge für eine Anpassung des Landesrechts vorgelegt und damit zahlreiche Anregungen für eine neuzeitlichere Gestaltung des Datenschutzes gegeben. Bedauerlicherweise wurde die gesetzgeberische Initiative im Wesentlichen auf die Anpassung an das EG-Recht beschränkt und damit die Chance für eine Modernisierung bislang nicht ausreichend genutzt.

Das Gesetz sieht zwar nunmehr eine verpflichtende Vorabkontrolle vor, mit der technische und organisatorische Maßnahmen vor dem erstmaligen Einsatz automatisierter Verfahren auf die damit verbundenen Gefahren für das Recht auf informationelle Selbstbestimmung untersucht werden sollen. In erster Linie ist dies eine Aufgabe des von der jeweiligen öffentlichen Stelle bestellten Datenschutzbeauftragten vor Ort. Leider ist die Verpflichtung öffentlicher Stellen, einen Datenschutzbeauftragten zu bestellen, nicht obligatorisch im Gesetz verankert worden, obwohl mehrere öffentliche Stellen einen gemeinsamen behördlichen Datenschutzbeauftragten bestellen können und es so möglich ist, den Aufwand für die Prüfung und den Einsatz ohnehin notwendiger Datenschutzmaßnahmen zu reduzieren. Auch bei meinen Kontrollen sind – was letztlich sogar im Interesse der im Blickpunkt stehenden öffentlichen Stelle liegen muss – sachkundige Ansprechpartner vonnöten. Diese haben oft nur faktisch die Rolle eines Datenschutzbeauftragten, ohne als solcher formell durch die Behördenleitung bestellt zu sein. Wünschenswert ist daher ein hoher Grad an Bestellungen von Datenschutzbeauftragten im Lande, damit öffentliche Stellen auch eine größere Sicherheit in der Umsetzung des Datenschutzrechtes erreichen.

Immer noch auf der Tagesordnung steht auch die Frage, ob die sinnvolle Zusammenlegung der Datenschutzkontrolle für den öffentlichen und den nicht-öffentlichen Bereich in Angriff genommen werden sollte.

Die Zusammenfassung der Datenschutzaufsicht bei dem Landesbeauftragten oder wie in Schleswig-Holstein in einer gemeinsamen Institution, der der Landesbeauftragte für Datenschutz vorsteht, ist – auch unter Berücksichtigung des Art. 28 I der Europäischen Datenschutzrichtlinie – sicherlich nicht in letzter Konsequenz zwingend erforderlich.

Sie wäre jedoch unter vielen Gesichtspunkten eine sinnvolle organisatorische Lösung. Die Zusammenfassung der Aufsichtskompetenz über den öffentlichen wie über den nicht-öffentlichen Bereich entspräche einerseits dem Geist der EG-Datenschutzrichtlinie und wäre andererseits auch im Hinblick auf die durch die entstehenden Synergieeffekte zu erreichende Steigerung der Effizienz in der Verwaltung außerordentlich zu begrüßen. Zumal – wie eine bundesweite Umfrage ergeben hat – die Aufsichtsbehörden der Länder personell nicht so besetzt sind, wie es die schnelle Entwicklung der Datenschutztechnologie und der damit gerade im nicht-öffentlichen Bereich vorhandene Kontrollbedarf erfordert.

Außerdem wäre die Zusammenfassung der Datenschutzaufsicht „in einer Hand“ eine überaus bürgerfreundliche Lösung. Nur eine einzige – zudem besser als die im ministeriellen Bereich angesiedelte Aufsicht als „Ombudsmann“ des Parlamentes für die Bürger bekannte – für alle Beschwerden zuständige Stelle wäre eine bürgerfreundliche Lösung, die im Sinne der Betroffenen die schwer einsehbaren Abgrenzungsprobleme zwischen dem öffentlichen und dem nicht-öffentlichen Sektor zur Vergangenheit macht.

Dies insbesondere auch mit Blick auf die unter dem Aspekt „Selbstdatenschutz“ immer wichtiger werdende Aufgabe der „Hilfe zur Selbsthilfe“, womit die Funktion des Datenschutzbeauftragten als Servicezentrum für die Bürgerinnen und Bürger gemeint ist.

Die im Grunde einzige Problematik bei der Lösung des Problems, ob denn nun die Zusammenlegung der beiden noch getrennten Datenschutzbereiche vorgenommen werden soll, ist, dass nicht mit letzter Sicherheit gesagt werden kann, ob das beim Landesbeauftragten vorhandene Personal ohne Zuwachs durch das im Geschäftsbereich der für den nicht-öffentlichen Bereich zuständigen Aufsichtsbehörde vorhandene bzw. weiteres Personal ausreicht, um den sich ergebenden Arbeitsanfall, der erfahrungsgemäß bei bekannt werden einer solchen Zusammenlegung an Umfang zunimmt, bewältigen zu können. Ich denke jedoch, dass es die Stärkung der durch den Datenschutzbeauftragten wahrgenommenen Kontrollmöglichkeit des Parlaments einerseits und die Verbesserung der Serviceleistungen für die Bürgerinnen und Bürger andererseits rechtfertigen, die Zusammenlegung der Datenschutzkontrolle dennoch vorzunehmen.

Es wäre auch zu begrüßen gewesen, wenn das so genannte „Datenschutzaudit“ eingeführt worden wäre. Dabei handelt es sich um ein Zertifikat, das den datenverarbeitenden Stellen für einen besonders herausgehobenen Datenschutzstandard und größtmögliche Datensparsamkeit verliehen wird. Ein solches Datenschutzaudit kann eine bessere und schnellere Kontrolle von Anwendungen in der Datenverarbeitung zur Folge haben.

Bundesweit ist eine „Zweite Stufe“ bei der Novellierung des Datenschutzrechtes geplant. Ich hoffe, dass im Zuge dieser Rechtsetzung eine Vereinfachung und Modernisierung des Datenschutzes gelingen wird.

3.2 Bekämpfung der Organisierten Kriminalität und des Terrorismus

Im Jahre 2001 wurde dem Landesamt für Verfassungsschutz (LfV) die neue Aufgabe übertragen, Bestrebungen und Tätigkeiten der Organisierten Kriminalität in der Bundesrepublik Deutschland zu beobachten. Dazu wurde die Befugnis eröffnet, besondere technische Mittel auch im Schutzbereich von Wohnungen einzusetzen. Durch das LfV dürfen nach dem jetzigen Gesetzeswortlaut sowohl akustische als auch optische Wohnraumüberwachungen durchgeführt werden. Im Zuge der Gesetzesänderung ist auch eine Bestimmung entfallen, wonach gesetzlich festgelegte Zeugnisverweigerungsrechte nicht beeinträchtigt werden durften.

Nicht bedacht wurde in diesem Zusammenhang, dass damit auch die besonderen Rechte der Berufsgeheimnisträger, wie beispielsweise Ärzte, Rechtsanwälte, Journalisten, Seelsorger, und anderer Personen, die im Strafverfahren und teilweise auch im präventiven Polizeibereich Zeugnisverweigerungsrechte innehaben, nicht mehr zu beachten waren. Dass die zuvor im Gesetz verankerten Zeugnisverweigerungsrechte entfallen sollten, hatte ich im Rahmen meiner Anhörung im Gesetzgebungsverfahren – entgegen anders lautenden Pressemitteilungen – durchaus zum Ausdruck gebracht.

Nunmehr wurde diese Frage im Zusammenhang mit der landesrechtlichen Umsetzung des Terrorismusbekämpfungsgesetzes erneut diskutiert und ein entsprechender Abänderungsantrag, mit dem die Beachtung der Zeugnisverweigerungsrechte für Berufsgeheimnisträger wieder eingeführt werden sollte, vorgelegt. Die Verabschiedung der gesetzlichen Änderung ist zwischenzeitlich erfolgt.

Nicht zu begrüßen ist allerdings im gleichen Gesetz die polizeirechtliche Bestimmung zur Rasterfahndung, mit der die Eingriffsschwelle für diese herausgehobene Ermittlungsmethode der Polizei herabgesenkt wurde.

Hier hatte ich empfohlen, angesichts der beim Bundesverfassungsgericht derzeit anhängigen Verfassungsbeschwerden zur Rasterfahndung und vor allem angesichts der vielfachen unbestimmten Rechtsbegriffe, die im Entwurf zur Rasterfahndungsbestimmung enthalten sind, mit den Überlegungen zu einer Gesetzesänderung zumindest so lange zuzuwarten, bis die verfassungsrechtliche Bewertung durch das höchste Bundesgericht vorliegt. Der eventuell vorzeitigen Verabschiedung einer zukünftig für verfassungswidrig erachteten Norm hätte damit vorgebeugt werden können, zumal die Zulässigkeit der bundesweiten Rasterfahndungen auf der Grundlage des jetzigen Gesetzeswortlautes durch die meisten gerichtlichen Entscheidungen bestätigt wurde.

Die Entscheidung des Bundesverfassungsgerichts bleibt abzuwarten.

3.3 Biometrische Merkmale in Personalausweisen und Pässen

Schon im Vorfeld der Verabschiedung des Terrorismusbekämpfungsgesetzes haben die Datenschutzbeauftragten des Bundes und der Länder die Pläne der Bundesregierung bewertet, neben dem Lichtbild und der Unterschrift weitere biometrische Informationen wie beispielsweise Fingerabdrücke, Handgeometrie, Gesichtsgeometrie in deutsche Personalausweise und Pässe aufzunehmen (Anlage 1). In der Folge wurde eingehend über Geeignetheit, Erforderlichkeit und Angemessenheit der beabsichtigten Einführung biometrischer Merkmale in Ausweisen und Pässen diskutiert. In einer zweiten Entschließung wurden dann nach Inkrafttreten des Terrorismusbekämpfungsgesetzes, das eine Regelung zu solchen Maßnahmen nunmehr enthält, weitere Anforderungen aufgestellt, damit auch datenschutzrechtlichen Erfordernissen in diesem Zusammenhang Rechnung getragen wird (Anlage 2).

3.4 Verstärkte „Indienstnahme Privater“

Es ist nicht zu übersehen, dass der Gesetzgeber und damit die öffentlichen Stellen zunehmend auf die Mitwirkung Privater setzen, um staatliche Ziele zu erreichen. Diese Tendenz zeigt sich vor allem im steuerlichen Bereich. Dort setzt sich eine fehlende Mitwirkung, wie beispielsweise nach dem Umsatzsteuergesetz (s.a. TZ 7.3), sogar in Sanktionen gegenüber demjenigen um, der sich nicht die Freistellungsbescheinigung seines Auftragnehmers vorlegen lässt, mit der nachgewiesen werden soll, dass dieser seinen Steuerpflichten nachgekommen ist. Wird die Kontrolle eines Vertragspartners versäumt, so führt dies schlimmstenfalls dazu, dass der Auftraggeber selbst die Steuerlast seines Auftragnehmers für dieses Vertragsverhältnis übernehmen muss. Auf den ersten Blick könnte man meinen, dass es sich hier nicht um Vorgänge handele, die das Recht auf informationelle Selbstbestimmung berührten. Dem ist jedoch nicht so; die Verpflichtung führt zu größerer Wachsamkeit und Beobachtungen anderer im Rechtsverkehr, wo die Beziehungen zum Staat bislang grundsätzlich Sache jedes einzelnen Vertragspartners waren und der Einzelne nicht noch Sorge zu tragen hatte für das rechtmäßige Verhalten eines Vertragspartners. Vor allem im Interesse einer Steuergerechtigkeit wird das bisher doch überwiegend herrschende Prinzip der Alleinverantwortlichkeit Einzelner gegenüber dem Staat zunehmend mehr durchlöchert.

Die Beispielsfälle häufen sich. Hatte man bislang als Verkäufer nur den Käufer eines Kraftfahrzeugs nach der Straßenverkehrszulassungsordnung dem Staat gegenüber zu offenbaren, so soll nach den Vorstellungen einer Kommune nunmehr auch der Käufer eines Hundes vom Verkäufer gegenüber dem Steueramt angegeben werden (s. TZ 7.1). Besonders gravierend ist die Veränderung des zwischenmenschlichen Klimas in Vertrauensbeziehungen, wenn Banken, Rechtsanwälte, Notare, Steuerberater und sogar Immobilienmakler in die staatliche Geldwäschebekämpfung miteinbezogen werden, wie dies in der jüngsten Änderung des Geldwäschegesetzes angeordnet wurde. Statt Vertrauen aufzubauen, wird zunächst einmal misstrauische Distanz gewahrt, da man die Daten des Ratsuchenden möglicherweise den Strafverfolgungsbehörden zu übermitteln hat.

Die Tendenz, Private, auch wenn sie nur vertragliche oder berufliche Kontakte geknüpft haben, zur gegenseitigen Kontrolle zu verpflichten, um dem Staat Angaben über eine andere Person machen zu können, darf sich nicht weiter fortsetzen.

Zu Recht wurde dies in der Presse bereits als „Indienstnahme Privater“ durch den Staat tituliert.

4 Justiz

4.1 Prüfung der Geschäftsstellen eines Amtsgerichts

Im Berichtszeitraum wurden die Geschäftsstellen eines Amtsgerichts überprüft, für die ich, soweit es sich um die Erfüllung von Verwaltungsaufgaben handelt, zuständig bin (§ 2 Abs. 1 Satz 4 SDSG).

Aufgrund meines Prüfberichts wurden einige Verbesserungen bei der Datenverarbeitung zugesagt. So sollte der Postraum für Rechtsanwälte entweder mit verschließbaren Fächern ausgestaltet werden, oder die Post in einem Raum deponiert werden, der bereits mit verschließbaren Fächern ausgestattet war. Aktenaussonderungsaktionen wurden angekündigt, da in einigen Bereichen die Aufbewahrungsfristen nicht beachtet worden sind. Eine Sammlung nicht anonymisierter Gerichtsentscheidungen soll es zukünftig ebenfalls nicht mehr geben. Aus bei einem anderen Amtsgericht konkret gegebenem Anlass habe ich auch auf die Notwendigkeit des Erlasses einer Fax-Dienstanweisung hingewiesen, die allen Bediensteten zur Kenntnis gebracht werden soll.

Zu den Unterlagen, die faktisch fast unbegrenzt aufbewahrt wurden, zählten die Protokoll- und Kassenbücher der Schiedsleute. Der Abschluss der Bücher erfolgte nicht nach einem bestimmten Zeitraum (z.B. ein Jahr) sondern nur dann, wenn ein Buch vollständig beschriftet war. Aufgrund des Umfanges der Bücher sowie der Anzahl der Fälle konnten sich Laufzeiten von mehreren Jahren für ein Buch ergeben.

Dies war unbefriedigend, weil die Bücher erst nach Abschluss dem zuständigen Amtsgericht übergeben und das Kassenbuch dort erst nach 10 Jahren sowie das Protokollbuch nach 30 Jahren vernichtet wurde.

Von Seiten der Behördenleitung wurde angeordnet, dass zum Ende des Jahres 2001 alle Protokoll- und Kassenbücher abzuschließen seien, die seit fünf und mehr Jahren im Gebrauch sind. Durch diese Bereinigung wird eine gewisse Abhilfe geschaffen, das Problem überlanger Aufbewahrungsfristen bei der Justiz ist damit allerdings noch nicht behoben (s. zuletzt 18. TB, TZ 5.2). Gemindert wird lediglich die Gefahr, dass Erkenntnisse aus Einzelfällen über Jahre hinweg bei den Schiedsleuten gespeichert bleiben, was in einer Eingabe moniert wurde, die jedoch nicht dieses Amtsgericht betraf.

Auf meinen Hinweis wurden des Weiteren die Geschäftsstellen und Protokollführer darauf aufmerksam gemacht, dass die Sitzungsrolle nicht den Verfahrensgegenstand, wie dies teilweise festgestellt wurde, enthalten soll.

Beim Einsatz der EDV soll zukünftig auf eine ordnungsgemäße Sicherung und frühzeitige Löschung der Dokumente geachtet werden. Das Aufstellen privater PC's darf nicht mehr zugelassen werden.

Im Hinblick auf die technisch-organisatorischen Voraussetzungen für den EDV-Einsatz gehe ich jedoch davon aus, dass die EDV-Koordinationsstelle beim Ministerium der Justiz alle Gerichte über die datenschutzrechtlichen Voraussetzungen einer elektronischen Datenverarbeitung unterrichtet und für deren praktische Umsetzung Sorge trägt.

4.2 Insolvenz- und Zwangsversteigerungsverfahren im Internet

Vorwiegend unter dem Gesichtspunkt der Kostenersparnis gegenüber Bekanntmachungen in Printmedien hat sich der Gesetzgeber für eine Veröffentlichung der Daten von Insolvenzschuldnern im Internet ausgesprochen.

Die Datenschutzbeauftragten des Bundes und der Länder haben schon in einem frühen Stadium auf die damit verbundenen Risiken für die Insolvenzschuldner hingewiesen, die zeitlebens weltweit abrufbar am Schulden-Pranger stehen können, obwohl dies keineswegs in der gesetzgeberischen Absicht gestanden hat. (s. Anlage 3) Das Insolvenzverfahren soll im Gegenteil in erster Linie zur Sanierung des Schuldners führen, so dass er nach einigen Jahren wieder in die Lage versetzt wird, unbelastet am Wirtschaftsverkehr teilzunehmen. Insofern ist eine Internetveröffentlichung diesem Ziel grundsätzlich abträglich.

Auf die Nachfrage des Ministeriums der Justiz, ob Internetveröffentlichungen über Insolvenz- und Zwangsvollstreckungsverfahren als zulässig angesehen werden, habe ich auf die in anderen Bundesländern aufgetretenen Probleme in diesem Zusammenhang hingewiesen. Abgesehen davon, dass in Zwangsvollstreckungsverfahren im Gegensatz zu Insolvenzverfahren keine normenklare Rechtsgrundlage für eine Internetveröffentlichung besteht, sind die Gefahren des Internets trotz der im Insolvenzverfahren geltenden Verordnung zu öffentlichen Bekanntmachungen im Internet vom 12.2.2002 (BGBl. I S. 677) von Seiten des Gesetz-/Verordnungsgebers nur sehr schwer begrenzbar.

Um Eingaben von Schuldnern, die ihre Datenschutzrechte einfordern, hierzulande zu vermeiden, habe ich dem Ministerium der Justiz empfohlen, eine Internetveröffentlichung für Insolvenz- und Zwangsvollstreckungsschuldner erst dann in die Wege zu leiten, wenn die damit zusammenhängenden Probleme umfassend gelöst sind.

Ich habe auch darum gebeten, den Vorschlag meiner nordrhein-westfälischen Kollegin und des Bundesbeauftragten für den Datenschutz, die Justizministerkonferenz mit der Thematik zu befassen, von Seiten des Saarlandes zu unterstützen.

4.3 Entscheidung des Bundesverfassungsgerichts zum Begriff „Gefahr im Verzug“ im Strafverfahren

Von grundlegender Bedeutung für die Staatsanwaltschaft aber auch die Polizei war im Jahre 2001 eine Entscheidung des Bundesverfassungsgerichts zu dem vom Gesetzgeber des Öfteren verwandten Begriffes der „Gefahr im Verzug“.

Der Datenschutz kann durch verfahrenssichernde Maßnahmen verstärkt werden. Zu diesen Maßnahmen zählt vor allem der Richtervorbehalt, wonach bestimmte, schwerwiegende Eingriffe in die Grundrechte nur nach einer richterlichen Überprüfung der gesetzlichen Voraussetzungen zulässig sein sollen. Um jedoch in Eilverfahren, in denen ein Richter nicht erreichbar ist, die Durchführung einer Maßnahme nicht zu gefährden, wird auch eine Zuständigkeit anderer Amtsträger öffentlicher Stellen, deren schnellere Verfügbarkeit unterstellt wird, gesetzlich angeordnet. Die Zuständigkeit dieser Stellen ist bei Vorliegen der sogen. „Gefahr im Verzug“ gegeben, deren Voraussetzungen das Bundesverfassungsgericht im Zusammenhang mit einer Wohnungsdurchsuchung in seiner Entscheidung vom 20.2.2001 (2 BVR 1444/00) ausführlich begründet hat.

Für den Datenschutz ist von besonderer Wichtigkeit, dass für den erheblichen Eingriff in die Privatsphäre eines Betroffenen, der stets mit Eingriffen in das Recht auf informationelle Selbstbestimmung verbunden ist, Verfahrenssicherungen aufgestellt wurden, wonach der Eilfall sowohl zu begründen als auch vor allem in der Akte nachvollziehbar zu dokumentieren ist. Letzterer Gesichtspunkt dient ebenso der etwaigen Durchführung einer datenschutzrechtlichen Kontrolle.

Ich begrüße es sehr, dass der Generalstaatsanwalt des Saarlandes hierzu Hinweise gegeben hat, deren datenschutzrechtlichen Gehalt ich wiedergeben möchte; an diese Hinweise sind sowohl die Staatsanwaltschaft als auch deren Hilfsbeamte (Polizei) im Strafverfahren gebunden.

Im Einzelnen wurden folgende Richtlinien gegeben:

- Der Begriff der „Gefahr im Verzug“ ist eng auszulegen.
- Die richterliche Anordnung muss die Regel und die nichtrichterliche Anordnung die Ausnahme sein. Die Strafverfolgungsbehörden müssen deshalb regelmäßig versuchen, eine Anordnung des instanziell und funktionell zuständigen Richters zu erlangen.
- Zu diesem Zweck müssen sowohl die Strafverfolgungsbehörden als auch die Ermittlungsrichter und die Justizverwaltung im Rahmen des Möglichen besondere tatsächliche und rechtliche Vorkehrungen treffen, die sicherstellen, dass die Regelzuständigkeit des Richters in der Praxis gewahrt wird. Dazu gehört auch die Einrichtung eines Eil- und Notdienstes bei den Gerichten.

- „Gefahr im Verzug“ ist dann – und zwar immer nur dann – anzunehmen, wenn die vorherige Einholung der richterlichen Anordnung den Erfolg der Durchsuchung gefährden würde, insbesondere wenn aufgrund der konkreten Umstände des Einzelfalles ansonsten ein Beweismittelverlust zu besorgen wäre und wenn der Gefahr des Beweismittelverlustes nur dadurch begegnet werden kann, dass die Strafverfolgungsbehörden sofort handeln.

- Die Annahme von „Gefahr im Verzug“ muss mit bestimmten Tatsachen begründet werden, die auf den Einzelfall bezogen sind. Reine Spekulationen, hypothetische Erwägungen und lediglich auf kriminalistische Alltagserfahrung gestützte fallunabhängige Vermutungen reichen nicht aus. Ebenso reicht die bloße Möglichkeit eines Beweismittelverlusts nicht aus.

- Die Annahme von „Gefahr im Verzug“ darf ferner nicht allein mit dem abstrakten Hinweis begründet werden, eine richterliche Entscheidung sei gewöhnlicherweise zu einem bestimmten Zeitpunkt oder innerhalb einer bestimmten Zeitspanne nicht mehr zu erlangen.

- Insbesondere dürfen die Strafverfolgungsbehörden die tatsächlichen Voraussetzungen für „Gefahr im Verzug“ nicht dadurch selbst herbeiführen, dass sie so lange mit dem Antrag an den Ermittlungsrichter zuwarten, bis dieser nicht mehr erreichbar ist und/oder Beweismittelverlust droht.

- Bei der Anwendung des Begriffs „Gefahr im Verzug“ handelt es sich nicht um eine Ermessensentscheidung. Den Behörden kommt in dieser Hinsicht auch kein Beurteilungsspielraum zu. Vielmehr handelt es sich um einen unbestimmten Rechtsbegriff, der der vollen – auch nachträglichen – gerichtlichen Überprüfung unterliegt.

- Deshalb müssen die Strafverfolgungsbehörden bei Annahme von „Gefahr im Verzug“ ihre Entscheidung in den Ermittlungsakten dokumentieren und begründen. Die Dokumentations- und Begründungspflicht hat nach Auffassung des BVerfG Verfassungsrang. Das BVerfG leitet sie aus Art. 19 Abs. 4 GG ab. Damit soll erreicht werden, dass der Eingriff messbar bleibt und die richterliche Kontrolle zumindest im Nachhinein als Instrument der Grundrechtssicherung praktisch wirksam werden kann, wenn sie schon im Vorhinein nicht durch Beachtung des Richtervorbehalts aktiviert wurde.

- Die Dokumentations- und Begründungspflicht ist daher unbedingt zu beachten. Das erfordert, dass der handelnde Beamte vor oder jedenfalls unmittelbar nach der Durchsuchung seine für den Eingriff bedeutsamen Erkenntnisse und Annahmen in den Ermittlungsakten dokumentiert. Dazu gehört, dass er den Tatverdacht und die gesuchten Beweismittel in einem Aktenvermerk so genau beschreibt, dass der äußere Rahmen abgesteckt ist, innerhalb dessen die Zwangsmaßnahme durchgeführt werden soll bzw. durchgeführt worden ist. Darüber hinaus muss er die Umstände darlegen, auf die er die Gefahr des Beweismittelverlusts stützt. Allgemeine Formulierungen, die den Begriff nur mit anderen Worten („Leerformeln“) oder nur die juristische Definition des Begriffs „Gefahr im Verzug“ wiedergeben, reichen nicht aus. Insbesondere muss erkennbar sein, ob der Beamte versucht hat, den zuständigen Richter zu erreichen. Die Dokumentation muss so vollständig sein, dass der handelnde Beamte im Falle einer richterlichen Nachprüfung seines Handelns auf die dokumentierten Tatsachen verweisen kann.

- Im Falle eines späteren gerichtlichen Verfahrens haben die Strafverfolgungsbehörden ihre Durchsuchungsanordnung zu begründen. Ihre Ausführungen müssen sich auf die gesetzlichen Voraussetzungen der Durchsuchung (§§ 102 ff. StPO) erstrecken. Außerdem müssen sie darlegen, warum eine richterliche Anordnung zu spät gekommen wäre, und gegebenenfalls, warum von dem Versuch abgesehen wurde, eine richterliche Entscheidung zu erlangen.

Die Entscheidung des Bundesverfassungsgerichts ist auch über die Maßnahme der strafprozessualen Durchsuchung hinaus von allen Stellen zu beachten, denen der Gesetzgeber eine so genannte Eilkompetenz bei „Gefahr im Verzug“ gewährt hat.

4.4 Anlasslose DNA-Analyse aller Männer

Im politischen Raum wurde im Zusammenhang mit einem Aufsehen erregenden Strafverfahren, in dem die Ermittlung des Täters Schwierigkeiten bereitete, die Forderung nach einer Regelung erhoben, wonach rein vorsorglich die gesamte männliche Bevölkerung der Bundesrepublik sich zur Identifikation einer DNA-Analyse unterziehen sollte. Da dies von politisch herausgehobener Stelle vertreten wurde, haben die Datenschutzbeauftragten des Bundes und der Länder es für geboten erachtet, in einer Entschließung die Unverhältnismäßigkeit und damit Verfassungswidrigkeit einer solchen Maßnahme zu betonen (Anlage 4).

4.5 Datenübermittlungen nach Kirchenaustritt

Erklärungen zum Austritt aus öffentlich-rechtlichen Religionsgemeinschaften werden im Saarland von den Amtsgerichten entgegengenommen. Diese leiten die Erklärung formularmäßig weiter an die jeweilige Religionsgemeinschaft, an das Meldeamt des jetzigen Wohnortes sowie bei „Verheirateten oder verheiratet Gewesenen“ an das Standesamt, das für die Eheschließung zuständig war, sofern die Religionszugehörigkeit im Familienbuch eingetragen ist. Diese drei Übermittlungsfälle sind in der Sondervorschrift für das Saarland zur Anordnung über Mitteilungen in Zivilsachen geregelt.

Die Erforderlichkeit der Übermittlung an die jeweilige Kirche und an das Meldeamt zum Zwecke der Ausstellung von Lohnsteuerkarten liegt auf der Hand.

Die Weitergabe des recht sensiblen Datums an das Standesamt erscheint hingegen fragwürdig. Daran ändert auch die Tatsache nichts, dass zum Zeitpunkt der Heirat auf Wunsch der Eheschließenden dieses Datum in das Familienbuch aufgenommen wird. Wegen der Freiwilligkeit der Angabe handelt es sich um ein Datum, für dessen Angabe ein überwiegendes staatliches Interesse nicht vorhanden ist, da ansonsten eine Erklärungspflicht bestünde. Jedermann kann sich also dafür entscheiden, seine Religionszugehörigkeit für den Eintrag im Familienbuch zu offenbaren oder diese nicht anzugeben.

Aus der Freiwilligkeit der Angabe muss andererseits bei einem Kirchenaustritt der Schluss gezogen werden, dass keine „Zwangsübermittlung“ an das Standesamt erfolgen darf, denn der Eintrag und demzufolge auch die Löschung liegt nicht im staatlichen Interesse.

Ich habe vorgeschlagen, dem Betroffenen die Übermittlung an das Standesamt nur mit seiner Einwilligung sozusagen als Serviceleistung durch die amtsgerichtliche Stelle anzubieten, die dieser zu diesem Zeitpunkt allerdings auch ablehnen kann.

Der Vorschlag erschien mir umso einsichtiger, als eine statistische Erklärungspflicht des Betroffenen ohnehin nach dem Personenstandsgesetz (§ 69a) vorgesehen ist. Diese besteht hingegen nur zu drei Zeitpunkten: Geburt eines Kindes, Eheschließung, Tod. Zu diesen Zeitpunkten könnten dann auch Berichtigungen erfolgen. An einer personengebundenen Speicherung ist der Staat zu diesen Anlässen außerdem nicht interessiert. Es werden dazu, wie im Gesetz vorgesehen, lediglich Zählkarten ausgefüllt, die aus Strichlisten bestehen.

Wenn lediglich die von staatlicher Seite als erforderlich angesehenen statistischen Erhebungszeitpunkte herangezogen würden, bliebe den Betroffenen auch bei der Erklärung des Kirchenaustritts die Vorlage ihres Familienbuches erspart, aus dem sich dieser Eintrag ergibt. Aus Anlass eines Kirchenaustritts ist die Kenntnisnahme des Geschäftsstellenbeamten beispielsweise über (mehrfache) Eheschließungen und Ehescheidungen nicht angemessen. Wie mir bei der Prüfung eines Amtsgerichtes dargelegt wurde, wird die Vorlage eines Familienbuchs jedoch verlangt, um überprüfen zu können, ob überhaupt ein Eintrag vorliegt, da dies den Betroffenen des Öfteren nicht mehr in Erinnerung sei.

Die freiwillige Angabe der Religionszugehörigkeit führt demnach dazu, dass tiefgreifende Einblicke in das Privatleben aus Anlass eines Kirchenaustritts möglich werden.

Aus datenschutzrechtlicher Sicht müsste hier eine Gleichbehandlung mit den Personen erfolgen, die es vorgezogen haben, eine freiwillige Angabe über ihre Religionszugehörigkeit zu unterlassen.

Die Datenübermittlung von Amts wegen sollte für beide Personenkreise gleichermaßen unterbleiben.

Das Ministerium der Justiz zeigte sich gegenüber meinem Vorschlag nicht aufgeschlossen. Mich konnte sein Hinweis auf die allgemeine Bereinigungspflicht des Standesbeamten aufgrund einer - in diesem Punkt nicht normenklaren - Rechtsverordnung zum Personenstandsgesetz nicht überzeugen. Ich hätte auch erwartet, dass in dieser Frage die Grundsätze der Religionsfreiheit nach Art. 4 GG / Art. 140 GG heranzogen worden wären. Nach Abs. 3 des Art. 136 der Weimarer Verfassung, der über Art. 140 GG Bestandteil unseres Grundgesetzes ist, haben Behörden „nur soweit das Recht nach der Zugehörigkeit zu einer Religionsgemeinschaft zu fragen, als davon Rechte und Pflichten abhängen oder eine gesetzlich angeordnete statistische Erhebung dies erfordert“.

Diese Voraussetzungen liegen im Hinblick auf die freiwillige Angabe der Religionszugehörigkeit nicht vor, so dass diese keine personenbezogene Zwangsübermittlung bei einem Kirchenaustritt zur Folge haben darf. Formale Gesichtspunkte einer Buchbereinigung erscheinen mir demgegenüber nachrangig, zumal der Staat sein statistisches Interesse, um das es hier allein gehen kann, durch das Ausfüllen von Zählkarten zu ausschließlich 3 Anlässen befriedigt sieht. Auf die Sensitivität dieses personenbezogenen Datums „Religionszugehörigkeit“ dessen Verarbeitung nach Art. 8 der EG-Datenschutzrichtlinie einer besonderen gesetzlichen Zulassung bedarf, und auf das Fehlen der Übermittlungsvoraussetzungen für Ausnahmefälle habe ich ebenfalls aufmerksam gemacht.

Gänzlich unverständlich war in diesem Zusammenhang der letzte Hinweis des Ministeriums der Justiz, die betreffende Person habe durch ihre freiwillige Angabe gegenüber dem Standesbeamten die Tatsache ihrer Religionszugehörigkeit „öffentlich“ im Sinne der EG-Datenschutzrichtlinie gemacht.

Zusammenfassend wäre festzuhalten, dass der Datenübermittlung an das Standesamt sowohl die Erforderlichkeit als auch insbesondere die gesonderte gesetzliche Grundlage für die Datenverarbeitung eines sensitiven Datums fehlt.

Die Thematik bedarf aus datenschutzrechtlicher Sicht einer erneuten Erörterung.

4.6 Eurojust

Neben der Institution „EUROPOL“, die der Zusammenarbeit aller Polizeien der EU-Staaten dient, haben die nationalen Justizverwaltungen auch eine Zusammenarbeit auf der Ebene der Staatsanwaltschaften geplant. Dazu hat der Europäische Rat die gemeinsame Stelle „EUROJUST“ beschlossen.

Die personenbezogenen Daten, die dort verarbeitet werden sollen, entsprechen in ihrer Sensitivität denjenigen Daten, die EUROPOL auf polizeilicher Ebene zur Verfügung stehen.

In einer Entschließung haben die Datenschutzbeauftragten des Bundes und der Länder die Voraussetzungen aufgestellt, die diese Großbehörde zu erfüllen hat, um datenschutzrechtlichen Anforderungen zu genügen (Anlage 5).

4.7 Änderung der Anordnung über Mitteilungen in Strafsachen (MiStra)

Im Rahmen einer geplanten Änderung der MiStra soll auch die von mir in meinem 17. TB (TZ 6.5) angesprochene Mitteilung über Wahlrechtsausschlüsse in dem entscheidenden Punkt geändert werden.

Ich habe es sehr begrüßt, dass der Entwurf für die Änderung der Nr. 12 MiStra nunmehr auch in einem Abs. 4 die Verpflichtung zur Mitteilung des Endzeitpunktes des Wahlrechtsausschlusses enthält. Damit würde die Anforderung eines Führungszeugnisses durch die Meldebehörde entfallen, durch das die Behörde zur Prüfung der Weiterspeicherung des Wahlrechtsausschlusses derzeit mehr Informationen enthält als sie benötigt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auch weitere grundsätzliche Hinweise zur geplanten Änderung der MiStra an den Vorsitzenden der Justizministerkonferenz gerichtet, die lt. dessen Mitteilung an den MiStra-Ausschuss weitergeleitet wurden.

Inhaltlich haben die Vorschläge der Datenschutzbeauftragten Prinzipien zum Gegenstand, die mehrere Mitteilungsanordnungen betreffen, über die jedoch keine Benachrichtigung an die Betroffenen erfolgt, so dass ihre Rechtschutzmöglichkeiten geschmälert werden. Über zweckändernde Datenübermittlungen aus dem Strafverfahren sollte der Betroffene unterrichtet werden. Wegen der individuellen Bewertung in diesen Fällen ist den Staatsanwälten und Richtern die Entscheidung über die Mitteilung vorzubehalten.

Entscheidungen sollten auch nicht als Ganzes sondern nur in den für den Empfänger erforderlichen Bestandteilen übermittelt werden.

Auch sollte bei Einstellung von Verfahren wegen Schuldunfähigkeit eine Angleichung an den Datenschutzstandard des Bundeszentralregisters (§ 11 BZRG) dahingehend erfolgen, dass ein nicht älter als 5 Jahre zurückliegendes Sachverständigengutachten vorhanden sein muss und der Tatvorwurf bis zu einem gewissen Grad geklärt ist. Die Benachrichtigung des Betroffenen über die Mitteilung darf auch hier nicht fehlen.

Ob der MiStra-Ausschuss diese Anregungen aufgreifen wird, war bei Redaktionsschluss noch offen.

4.8 Verwertung von Daten aus Telefonaten außerhalb des Strafverfahrens

Manche Eingaben von Petenten finden erst Jahre später eine Fortsetzung. So hatte der Petent, der sich im Berichtszeitraum 1993/1994 wegen der Auswirkungen einer gegen ihn gerichtete Telefonüberwachungsmaßnahme an mich gewandt hatte (15. TB, TZ 4.2) erneut Anlass, um datenschutzrechtlichen Rat zu bitten.

Nunmehr sollten die Telefonüberwachungsunterlagen, die einer privaten Versicherung damals von der Staatsanwaltschaft zur Verfügung gestellt wurden, in einem Zivilprozess Verwendung finden.

Die Problematik der Einsichtnahme durch eine private Versicherung habe ich im 15. Tätigkeitsbericht dargestellt. Anfang des Jahres 2001 konnte ich den Petenten darüber informieren, dass der Gesetzgeber im Strafverfahrensänderungsgesetz 1999, das gegen Ende des Jahres 2000 in Kraft getreten ist, eine Verwendungsbeschränkung für Daten aus so genannten verdeckten Maßnahmen im Strafverfahren angeordnet hat. Zu den verdeckten, d.h. ohne Kenntnis des Betroffenen vorgenommenen Maßnahmen zählt auch die Telefonüberwachung.

Informationen, die aus diesem Vorgehen gewonnen werden, dürfen nur für Zwecke eines Strafverfahrens, zur Abwehr von erheblichen Gefahren und für die Zwecke, für die eine Übermittlung nach § 18 des Bundesverfassungsschutzgesetzes zulässig ist, übermittelt werden (§ 477 Abs. 2 Satz 2 StPO).

Der Zweck, prozessuale Interessen vor dem Zivilgericht zu wahren, ist vom Normzweck demnach nicht umfasst.

Aus der Sicht des Datenschutzes durfte eine Verwertung der aus der Telefonüberwachung herstammenden Daten nicht stattfinden.

Wie der Petent mitgeteilt hat, wurden die Unterlagen aus der Telefonüberwachung im Zivilprozess daher auch nicht verwertet.

Die gleichen Prinzipien hat das Bundesverfassungsgericht unlängst in seinem Beschluss vom 9.10.2002 (1BvR 1611/96 und 1BvR 805/98) für die zivilgerichtliche Verwertung von privat erlangten Zeugenaussagen aufgestellt, wonach heimliches Mithören des nicht öffentlich gesprochenen Wortes bei einem Telefonat zur Unverwertbarkeit von Aussagen lauschender Zeugen führen kann. Das Gericht hat hervorgehoben, dass das allgemeine Interesse an einer funktionstüchtigen Straf- und Zivilrechtspflege sich nicht grundsätzlich gegen das allgemeine Persönlichkeitsrecht durchsetze. Allein das Interesse, sich ein Beweismittel für zivilrechtliche Ansprüche zu sichern, reiche daher nicht aus, um das Persönlichkeitsrecht nachrangig werden zu lassen.

4.9 Datenschutz im Strafvollzug

Im Strafvollzug kommt dem Datenschutz eine besondere Bedeutung zu, da es gilt, die widerstreitenden Interessen zwischen dem Persönlichkeitsrecht des Betroffenen und der Erfüllung der Vollzugsaufgaben in eine „praktische Konkordanz“ zu bringen. Dass dies zunächst nicht immer gelingt, zeigen auch in diesem Berichtszeitraum mehrere Eingaben von Gefangenen, die sich mit verschiedenen datenschutzrechtlichen Fragen im Zusammenhang mit dem Strafvollzug befassen.

Datenumfang des Einkaufsscheins

Der Einkaufsschein, der den Gefangenen berechtigt, einmal im Monat persönliche Artikel bei einer privaten Firma in der Justizvollzugsanstalt einzukaufen, enthielt den Namen des Gefangenen, dessen Geburtsdatum, die Vollzugsabteilung, eine Buchnummer, die das Jahr enthält, seit dem der Gefangene in der jeweiligen Anstalt einsitzt sowie den zur Verfügung stehenden Geldbetrag. Für die Durchführung und Abwicklung des Einkaufs sind Namen und Geburtsdatum nicht erforderlich, so dass bei der Ausstellung des Einkaufsscheins darauf verzichtet werden sollte. Da das derzeit in der Justizvollzugsanstalt eingesetzte Automationsverfahren die Unterdrückung dieser Angaben nicht unterstützt, wurde seitens der Justizvollzugsanstalt in einem „Probelauf“ getestet, ob eine eindeutige Zuordnung der Gefangenen aufgrund der Buchnummer sowie einer Wartemarke ausreichend ist. Die übrigen Angaben – insbesondere Name und Geburtsdatum – durften die Gefangenen schwärzen. Nach Auskunft der Justizvollzugsanstalt hat sich das Verfahren als praktikabel erwiesen, so dass beabsichtigt ist, weiterhin so zu verfahren. Beim Neudruck der Einkaufslisten sollten die Gefangenen durch einen Hinweis auf diese Möglichkeit hingewiesen werden.

Ich sehe dieses Verfahren zwar als Schritt in die richtige Richtung an, jedoch sollte der Einkaufsschein die nicht erforderlichen Daten von Anfang an nicht mehr enthalten. Eine Anpassung des automatisierten Verfahrens sollte dies gewährleisten.

Abschließbare Schränke in Haftzellen mit mehreren Insassen

Bisher war nur vereinzelt die Möglichkeit gegeben, persönliche Dinge wie z.B. private Post, Gerichts- und Anwaltspost, in einem verschließbaren Schrank oder sonstigen verschließbaren Behältnis in Gemeinschaftszellen gegen unbefugte Kenntnisnahme insbesondere durch Mitgefangene zu schützen. Wollte der Gefangene eine unbefugte Kenntnisnahme ausschließen, musste er die persönlichen Dinge verschlossen zu seiner Habe geben, die außerhalb der Zelle von der Justizvollzugsanstalt aufbewahrt wird. Auch wenn der Zugriff darauf in der Regel binnen Tagesfrist möglich war, hat diese Handhabung auf jeden Fall den uneingeschränkten Zugang erschwert. Wegen des einfacheren Zuganges für den Gefangenen selbst ist im Einzelfall nicht ausgeschlossen, dass doch persönliche Unterlagen unverschlossen in der Gemeinschaftszelle aufbewahrt werden.

Die Justizvollzugsanstalt erkennt meine Bedenken an und ist bemüht, nach und nach sämtliche mehrfach belegten Hafträume mit abschließbaren Spinden auszustatten. Es ist deshalb davon auszugehen, dass sich dieses Problem in absehbarer Zeit erledigt haben dürfte.

Einsatz von Gefangenen innerhalb der Justizvollzugsanstalt

Der Einsatz von Gefangenen bei der Wahrnehmung von Aufgaben der Justizvollzugsanstalt ist datenschutzrechtlich problematisch, wenn mit der Tätigkeit die Möglichkeit der Einsicht in personenbezogene Daten von Mitgefangenen besteht. So wurden im Rahmen einer Sportgemeinschaft der Justizvollzugsanstalt Gefangene mit der Abrechnung von Geldern der Mitgefangenen betraut und erhielten dadurch Zugang zu den kompletten Mitgliedslisten, die z.B. Namen, Adressen und Bankverbindungen enthielten.

Das Ministerium der Justiz teilte die datenschutzrechtlichen Bedenken gegen den Einsatz und hat inzwischen angeordnet, dass Mitgliederdaten der Sportgemeinschaft nicht mehr durch Gefangene verwaltet werden dürfen.

5 Polizei

5.1 Rasterfahndung

Wie die meisten Bundesländer so hatte auch die Polizei des Saarlandes als Folge der Anschläge vom 11.9.2001 in den USA eine Rasterfahndung im Land angeordnet.

Diese ist nach der entsprechenden Bestimmung des Saarländischen Polizeigesetzes zur Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib und Leben oder Freiheit einer Person zulässig. Unterschiedliche Entscheidungen in der Rechtsprechung zum Vorliegen einer „gegenwärtigen Gefahr“ hatten zunächst zum Aussetzen der Rasterfahndung in einem Bundesland geführt, die später jedoch fortgeführt wurde, nachdem eine letztinstanzliche Entscheidung in einem der Bundesländer ergangen ist und in anderen Bundesländern erst die dazu erforderlichen Rechtsgrundlagen zur Rasterfahndung geschaffen wurden.

Im Saarland ist – im Gegensatz zu einigen anderen Bundesländern – eine spezielle Anordnung der Rasterfahndung durch den Richter gesetzlich nicht vorgesehen. Die Anordnung ergeht durch den Behördenleiter, der Landesbeauftragte für Datenschutz ist hierüber zu unterrichten.

Nachdem die Anordnung und gleichzeitig auch meine Unterrichtung durch den Leiter der Behörde erfolgt sind, habe ich frühzeitig auf die Risiken dieser gesetzlich abgesicherten, aber dennoch umstrittenen, polizeilichen Ermittlungsmethode hingewiesen. Da bei der Rasterfahndung eine Vielzahl von personenbezogenen Daten aus eigenen Beständen der Polizei aber auch aus externen Quellen und nach einem festgelegten Muster untereinander abgeglichen werden, gerät eine große Zahl von Bürgern durch den Abgleich in das Blickfeld der Polizei.

Ich habe alle involvierten öffentlichen Stellen darauf aufmerksam gemacht, dass innerhalb der Gruppe derjenigen Personen, die dem bundeseinheitlich erstellten „Täterprofil“ entsprechen, sich eine Vielzahl von Mitbürgern befinden, die möglicherweise seit Jahren unbescholten im Saarland leben und denen es in der Vergangenheit fern gestanden hat und auch zukünftig fern stehen wird, terroristische Anschläge zu verüben. Für diese beruht der Treffer aufgrund des Täterprofils auf Zufälligkeiten. Sie bedürfen eines verstärkten Datenschutzes. Bewertungen und Auswertungen obliegen insofern ausschließlich den dafür zuständigen Gefahrenabwehrbehörden. Da das Instrument der Rasterfahndung die Gefahr von zunächst undifferenzierten Gruppenverdächtigungen in sich birgt, habe ich darum gebeten, bei der Datenverarbeitung größtmögliche Sorgfalt walten zu lassen. Die mit dem Abgleich befasste Organisationseinheit muss auch innerhalb der öffentlichen Stelle so abgeschottet sein, dass Unbefugten eine Kenntnisnahme der Trefferfälle nicht möglich und die informationelle Gewaltenteilung innerhalb der Verwaltung gewährleistet ist.

Es war nicht zuletzt zu bedenken, dass es sich bei der vorliegenden Rasterfahndung um die in Art. 8 EG-Datenschutzrichtlinie besonders geschützte und nur in Ausnahmefällen zulässige Datenverarbeitung über Daten rassischer und ethnischer Herkunft, religiöser oder philosophischer Überzeugungen gehandelt hat.

Wegen der höheren Sensibilität der Datenbestände war auch dafür Sorge zu tragen, dass die Datenbestände nur selektiert und die Datenträger besonders gesichert (von Hand zu Hand per eigenem Kurier oder dem des Landeskriminalamtes bzw. verschlüsselt) übergeben wurden.

Nach den Terroranschlägen haben sich die Datenschutzbeauftragten des Bundes und der Länder in Entschließungen (Anlagen 6 und 7) zu den Gefahren geäußert, die für die Freiheits- und Persönlichkeitsrechte Einzelner entstehen können, wenn der Gesetzgeber eine sachliche und verantwortungsbewusste Abwägung mit anderen staatlichen Zielvorgaben vermissen lässt. Entsprechende nicht mehr als verhältnismäßig anzusehende Vorschläge aus dem gesetzgeberischen Raum hatten dazu begründeten Anlass gegeben.

Über die Datenverarbeitung bei der saarländischen Polizei habe ich mich vergewissert und konnte zum damaligen Zeitpunkt keine Vorkommnisse erkennen, die mit der gesetzlichen Grundlage im Polizeirecht nicht im Einklang gestanden hätten. Allerdings musste ich nachträglich feststellen, dass auch die oberste Luftfahrtbehörde beim Ministerium für Wirtschaft Daten aus ihrem Bestand an das Landeskriminalamt übermittelt hat, die dort gerastert wurden, oder aber unmittelbar zwecks Rasterung an das Bundeskriminalamt weitergeleitet wurden. Meine erforderliche Unterrichtung ist in diesem Zusammenhang unterblieben, obwohl hier eindeutig ein Rasterfahndungsvorgang stattgefunden hat und das Landeskriminalamt insofern die gesetzliche Verpflichtung zur Unterrichtung gehabt hätte. Zudem hätte es einer Erweiterung der Rasterfahndungsanordnung bedurft.

Die Daten wurden überwiegend bundesweit nach dem Abgleich in den Bundesländern an das Bundeskriminalamt zwecks Koordinierung der Ermittlungen der Länderpolizeien übermittelt. In einigen Wochen soll nach Information des Landeskriminalamtes auch dort die Rasterfahndung beendet werden, so dass die Daten aller Personen, die nicht zu den konkret Verdächtigen zählen, auch beim BKA zu löschen wären.

5.2 Reportagen über polizeiliches Handeln

Spektakuläre Fälle, die die Polizei beschäftigen, finden auch großes Interesse bei den Medien. Dies ist nur allzu verständlich und entspricht auch im Regelfall dem berechtigten Informationsinteresse der Öffentlichkeit, so dass insbesondere Personen der Zeitgeschichte diese Darstellungen hinzunehmen haben, wenngleich auch Prominente hin und wieder ihre Persönlichkeitsrechte verletzt sehen und sie vor den Gerichten nicht selten obsiegen.

Eindeutig nicht akzeptabel ist indes, dass bei der Verfolgung kleinerer Verstöße gegen die Rechtsordnung, die so genannte einfache Bürger und Bürgerinnen begangen haben, Medienvertretern von Seiten der Polizei gestattet wird, an Amtshandlungen gegenüber Betroffenen teilzunehmen. Es ist hier zwar die Absicht erkennbar, polizeiliches Handeln in der Realität darstellen zu können, dies darf jedoch nicht soweit führen, dass personenbezogene Ermittlungen miterlebt werden, denn es handelt sich hierbei um Datenerhebungen, die nur der Polizei zur Kenntnis gelangen dürfen.

In einem Presseartikel der Saarbrücker Zeitung vom 4.12.02 habe ich zu meinem Erstaunen gelesen, dass ein Reporter die Polizei bei einer „Fahrer-Ermittlung“ begleitet hat. Die private Wohnungstür wurde – aus der Sicht des Datenschutzes – zum Glück nicht geöffnet. Die Wohnungsinhaber wären vermutlich zu Recht sehr ungehalten gewesen, wenn eine polizeiliche Befragung im Beisein eines Pressevertreters stattgefunden hätte.

In der Vorausschau eines solchen Geschehens habe ich in diesem Zusammenhang die „Verhaltensgrundsätze für Presse/Rundfunk und Polizei bei der Durchführung polizeilicher Aufgaben und der freien Ausübung der Berichterstattung“ vor allem zu einem dort geregelten Grundsatz moniert. Hier ist in Nr. 9 der Verhaltensgrundsätze die Feststellung enthalten:

> „Das Fotografieren und Filmen polizeilicher Einsätze unterliegt grundsätzlich keinen rechtlichen Schranken.“

Diese allgemeine Aussage ist mit dem Datenschutzrecht nicht zu vereinbaren. Sobald ein polizeilicher Einsatz einen Personenbezug erhalten kann, so zum Beispiel Identitätsfeststellungen zu treffen sind, werden Amtsgeheimnisse offenbart, die gleichzeitig dem Datengeheimnis unterliegen.

Für mich nicht verständlich war die offizielle Reaktion des Ministeriums für Inneres und Sport, als ich auf diesen unvertretbaren Satz in den Verhaltensgrundsätzen für Presse/Rundfunk und Polizei hingewiesen habe. In der Stellungnahme wurde betont, man gehe davon aus, die Medien selbst würden in verantwortlicher Weise die rechtlichen Vorgaben beachten. Die Wahrung der Amtsgeheimnisse ist hingegen nicht Angelegenheit der Medien sondern der öffentlichen Stellen, die bei Gefahren für das Recht auf informationelle Selbstbestimmung eine Teilnahme von Medienvertretern an Amtshandlungen, insbesondere solchen der Polizei, nicht zulassen dürfen. Das faktische Beispiel belegt, dass auch die Verhaltensgrundsätze für die Polizei im Umgang mit den Medien datenschutzrechtliche Risiken aufzuzeigen haben, damit der Umgang mit den Medien nicht in völlige Sorglosigkeit im Hinblick auf die informationelle Selbstbestimmung von Bürgern und Bürgerinnen abgleitet.

Der erste Schritt in Richtung Wahrung der Datenschutzrechte wäre insofern die Streichung des von mir gerügten Satzes in den Verhaltensgrundsätzen für die Polizei. Auf einer zutreffend formulierten abstrakten Grundlage sind solche tatsächlichen Vorkommnisse dann auch eher zu verhindern.

5.3 Personengebundene Hinweise in INPOL

Ein Petent hatte sich darüber beschwert, dass so genannte „personenbezogene Hinweise“ offenbar ein „Eigenleben“ führten.

In einer Datei der Polizei dürfen zu bereits vorhandenen Daten einer Person nach dem Gesetz Hinweise gespeichert werden, die zum Schutz dieser Person oder zur Eigensicherung von Beamten erforderlich sind (§ 7 Abs. 3 Bundeskriminalamtgesetz).

Im konkreten Fall hatte die Polizei (des Bundes oder eines Landes) zu einem später nicht mehr nachvollziehbaren Zeitpunkt zur Person des Petenten den Hinweis „bewaffnet und gewalttätig“ in ihre Verbunddatei – INPOL – aufgenommen, die von jedem Sachbearbeiter bei der Polizei bundesweit abgerufen werden kann.

Diese Vorgehensweise ist zwar im Hinblick auf den Hinweis „bewaffnet und gewalttätig“ von der Bestimmung des Bundeskriminalamtgesetzes gedeckt, denn diese Warnung ist für den Eigenschutz der Beamten bei einem Einsatz gegen die Person wichtig, um entsprechende Vorkehrungen im Umgang mit dem Täter treffen zu können.

Anlass für das Setzen dieses Hinweises im Verbundsystem kann indes nur eine Straftat sein, bei der der Täter sich als bewaffnet und gewalttätig gezeigt hat. Problematisch wird der Hinweis jedoch stets, wenn die Täterschaft nicht eindeutig festgestellt werden kann und es nicht zu einer gerichtlichen Verurteilung kommt, so dass eine Einstellung des Verfahrens erfolgen muss.

Im Beispielsfall konnte die Täterschaft zu einem vor Jahrzehnten begangenen Raubüberfall nicht dem Petenten mit rechtlicher Sicherheit angelastet werden. Aus dieser Zeit stammte jedoch der Hinweis, der damals dem in Verdacht geratenen Petenten zugeordnet wurde und der Begehensweise der Straftat „Raub“ auch immanent ist.

Nach der ständigen höchstrichterlichen Rechtsprechung darf die Polizei auch solche Daten über ehemals Verdächtigte weiterspeichern, bei denen ein polizeilicher „Restverdacht“, selbst nach einer Beendigung des Verfahrens ohne Verurteilung verbleibt.

Im Hinblick auf die Weiterspeicherung von Delikten aus Restverdachtsfällen ist jedoch ein strukturelles Defizit insofern erkennbar, als der zum Anlass eines Verdachtsfalles zutreffend gespeicherte personenbezogene Hinweis, losgelöst von diesem Delikt, manuell auch nach Löschung des Deliktes weitergespeichert werden kann. Das hat im dargestellten Fall dazu geführt, dass für den diskriminierenden Hinweis ,“bewaffnet und gewalttätig“ kein erforderlicher aktenmäßiger Bezug weder bei der Landes- noch bei der Bundespolizei vorhanden war, der Hinweis jedoch Einzug in eine neue Akte der Staatsanwaltschaft gefunden hatte, die allerdings außer diesem Hinweis keine Rechtfertigung für die Speicherung der Daten enthielt.

Die Lösung des Problems könnte darin gesehen werden, dass eine Löschung des Verdachtsfalles stets auch mit einer Löschung des personengebundenen Hinweises verbunden sein muss, sofern nicht ein neuer Verdacht-/Verurteilungsfall diese Etikettierung einer Person wiederum erlaubt.

Der saarländischen Polizei wäre ich für eine dahingehende Initiative und Erörterung in den Bund/Länder-Gremien zum INPOL-System verbunden.

5.4 Dokumentation der lagebildabhängigen Kontrollen

Über die Änderung des Saarländischen Polizeigesetzes (SPolG), die Anfang des Jahrs 2001 in Kraft getreten ist, habe ich bereits in meinem 18. TB, TZ 6.1, ausführlich berichtet.

Durch die Gesetzesänderung wurde unter anderem die „lagebildabhängige Kontrolle“(§ 9 a SPolG) als neue Befugnis für die Polizei im Gesetz verankert.

Um die Einhaltung der gesetzlichen Voraussetzungen dieses neuen polizeilichen Instrumentes überprüfen zu können, habe ich mich nach der Anzahl und der Effektivität der durchgeführten Kontrollen erkundigt. Für die Antwort auf meine Nachfrage zum Ende des Jahres 2001, die den Inhalt hatte, es lägen bislang keine aussagekräftigen Ergebnisse der lagebildabhängigen Kontrollen vor, konnte ich noch Verständnis aufbringen, da der Zeitraum ab Inkrafttreten der Bestimmung nicht einmal ein Jahr umfasst hat.

Unverständlich war hingegen der Hinweis, man habe bei bestimmten Dienststellen aufgrund dort bekannter Brennpunkte in diesem Zeitraum 60 Kontrollmaßnahmen durchgeführt, die allesamt nicht dokumentiert worden seien.

Das Verfahren kann in dieser Weise nicht beibehalten bleiben.

Die lagebildabhängige Kontrolle, bei der fast im gesamten Land jedermann von der Polizei angehalten und nach seiner Identität befragt werden kann, wobei z.B. der Kofferraum eines Fahrzeugs oder eine Aktentasche für den Blick des Polizeibeamten zu öffnen sind, muss nicht zuletzt für die Datenschutzkontrolle überprüfbar gehalten werden. Dies setzt zwingend eine Dokumentation über die Durchführung der polizeilichen Kontrollen voraus; das Lagebild muss hier in erster Linie die Rechtfertigung für den Eingriff in die Persönlichkeitsrechte darstellen. Dies gilt umso mehr, als die Betroffenen durch ihre Person keinen konkreten Anlass für die Eingriffsmaßnahmen der Polizei gegeben haben. Dass hier der Grundsatz aufgegeben wird, der herkömmlich polizeiliches Handeln an bestimmte Gefährdungen und Anhaltspunkte beim Betroffenen selbst bindet, darauf habe ich auch in einer Presseerklärung zum Gesetzentwurf aufmerksam gemacht.

Auch die Zweckbestimmung der für den Einzelnen anlasslosen Kontrolle muss überprüfbar bleiben. Nach dem Gesetz soll die Maßnahme dem Ziel dienen, die grenzüberschreitende Kriminalität bis zu einer Tiefe von 30 km von den Außengrenzen zu Frankreich und Luxemburg zu bekämpfen.

Anlasslose Kontrollen der Polizei, die keinen Bezug zu grenzüberschreitender Kriminalität aufweisen, sind mithin nicht zulässig.

Um berechtigte Kritik – etwa aus den Reihen betroffener Bürger – gar nicht erst aufkommen zu lassen, ist es daher geboten, die lagebildabhängigen Kontrollen anhand ihrer gesetzlichen Voraussetzungen eingehend zu dokumentieren.

5.5 Aussonderungsprüffrist bei Heranwachsenden

Mit dem Ministerium des Inneren und der Polizei wurde ein Schriftwechsel darüber geführt, wie lange personenbezogene Daten von Heranwachsenden in den Informationssystemen der Polizei nach Beendigung eines Verfahrens gespeichert bleiben sollten.

Bei den Heranwachsenden handelt es sich nach der strafrechtlichen Definition um die Altersgruppe der 18-21Jährigen. Ihnen billigt der Strafgesetzgeber im Jugendgerichtsgesetz (§§ 105, 106 JGG) Milderungen bei Bestrafungen zu, wenn

- die Gesamtwürdigung der Persönlichkeit des Täters bei Berücksichtigung auch der Umweltbedingungen ergibt, dass er zur Zeit der Tat nach seiner sittlichen und geistigen Entwicklung noch einem Jugendlichen gleichstand, oder
- es sich nach der Art, den Umständen oder den Beweggründen der Tat um eine Jugendverfehlung handelt.

In Erkenntnis der Tatsache, dass die weit überwiegende Anzahl der Verfahren Heranwachsender durch die Gerichte nach Jugendstrafrecht behandelt werden, habe ich vorgeschlagen, dass auch die Polizei bei der Weiterspeicherung von Daten aus diesen Verfahren die Fristen beachten soll, die für die Speicherung der Daten von Jugendlichen gelten. Die Prüffrist für Erwachsene beträgt nach dem Polizeigesetz 10 Jahre, diejenige für Jugendliche hingegen 5 Jahre. Eine eigene Prüffrist für Heranwachsende sieht das Gesetz nicht vor.

Es stellt sich demnach vorab die Frage, welcher Gruppe die Heranwachsenden bei der Prüfung einer Weiterspeicherung der Daten zuzuordnen sind. Mir erscheint die generelle Zuordnung der Heranwachsenden zu den Erwachsenen, angesichts der zusätzlichen Erkenntnis, dass die Gerichte im Regelfall das Jugendstrafrecht anwenden, nicht angemessen, weil die Verdoppelung der Speicherungsdauer, die für Daten Jugendlicher gelten, eine inkonsequente Verschärfung der Behandlung Heranwachsender bei der Polizei darstellt. Ich sehe hier einen auffälligen Gegensatz zum gerichtlichen Verfahren. Aus der Sicht des Datenschutzes wäre ein Gleichklang herzustellen, da sachgerechte Gesichtspunkte für ein verstärktes und verlängertes Informationsbedürfnis der Polizei bei Heranwachsenden im Vergleich zu Jugendlichen, wenn beide Gruppen nach gerichtlicher Wertung dem Jugendstrafrecht unterfallen, nicht erkennbar ist.

Der von gerichtlicher Nachsicht getragene Persönlichkeitsschutz für Heranwachsende sollte sich bei der Behandlung dieser Altersgruppe durch die Polizei fortsetzen.

6 Verfassungsschutz

6.1 Novellierung des Art. 10-Gesetzes

Im Berichtszeitraum wurde das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses nach Art. 10 GG novelliert. Dabei zu beachtende datenschutzrechtliche Anforderungen haben die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung festgehalten (Anlage 8).

Wie ich in meinem 18. TB, TZ 7.1 bereits dargestellt hatte, war einer der zentralen Punkte die lückenlose Kontrolle der Datenverarbeitung entweder durch die G 10 Kommission oder aber die Datenschutzbeauftragten in den Ländern. Im Art. 10-Gesetz hat sich der Bundesgesetzgeber dafür entschieden, der G 10 Kommission die Kontrolle der gesamten Erhebung, Verarbeitung und Nutzung der Daten zu übertragen. Ebenso beabsichtigt auch der Landesgesetzgeber, wie dem mir vorgelegten Entwurf eines Durchführungsgesetzes zum Art. 10-Gesetz im Rahmen der Terrorismusbekämpfung zu entnehmen ist, die G 10 Kommission des Landes mit der Kontrolle der gesamten Datenverarbeitung zu befassen. Nach dem Entwurf kann dem Landesbeauftragten für Datenschutz durch die Kommission allerdings Gelegenheit zur Stellungnahme in Fragen des Datenschutzes gegeben werden; insofern entspricht die Entwurfsregelung ebenfalls dem bereits geltenden Bundesrecht.

Anders als im Bundesrecht ist im Entwurf des Landesrechts leider nicht ausdrücklich geregelt, dass der Kommission Mitarbeiter mit technischem Sachverstand zur Verfügung zu stellen sind. Da diese beim Landesbeauftragten für Datenschutz vorhanden sind, könnte sich in diesem Bereich die Gelegenheit zur Stellungnahme durch meine Dienststelle ergeben.

Wesentlich ist in diesem Zusammenhang allerdings allein die Lückenlosigkeit der Datenschutzkontrolle sowohl in technischer, rechtlicher und nicht zuletzt faktischer Hinsicht, weil die Maßnahmen ohne Kenntnis der Betroffenen durchgeführt werden und die Kontrollen vor der Benachrichtigung des Betroffenen die Rechtsschutzmöglichkeiten zu ersetzen haben.

7 Steuern

7.1 Ersuchen des Steueramtes um Übermittlung von Listen der Hundeerwerber

Eine saarländische Stadt hat vom Betreiber eines privaten Tierheims seit Jahren die Listen der Kunden verlangt und auch erhalten, die einen Hund erworben haben. Nachdem Hundeerwerber sich darüber beschwert hatten, dass ihr Name und ihre Anschrift an das Steueramt der Stadt weitergegeben wurden, habe ich die Stadt um Stellungnahme zu dieser Verfahrensweise gebeten. Diese hat mir mitgeteilt, ein spezifisches Hundesteuergesetz, wie in einigen anderen Bundesländern, gäbe es im Saarland nicht; nach dem Kommunalabgabengesetz seien die Gemeinden jedoch verpflichtet, eine Hundesteuer zu erheben und die Einzelheiten in einer kommunalen Satzung zu regeln. In der städtischen Satzung habe man den bisherigen Hundehalter verpflichtet, Name und Anschrift des Erwerbers eines Hundes anzugeben.

Mir hat sich die Frage gestellt, ob eine derartige Verpflichtung zu einem Eingriff in das Recht auf informationelle Selbstbestimmung eines Hundeerwerbers durch eine kommunale (Steuer-)Satzung begründet werden darf. Die Beschwerdeführer sehen sich durch die Angabe ihrer personenbezogenen Daten, die ihr Partner aus einem privaten Vertrag an das Steueramt weiterzugeben hat, vorzeitig als mögliche „Steuersünder“ angeprangert.

Meiner rechtlichen Bewertung lagen folgende Überlegungen zugrunde, die ich sowohl dem Innen- als auch dem Finanzministerium dargelegt habe:

- Daten sind grundsätzlich beim Betroffenen zu erheben.
- Ausnahmen vom Grundsatz der Datenerhebung beim Betroffenen bedürfen einer ausdrücklichen Rechtsgrundlage, die dies vorsieht oder zwingend voraussetzt.
- Die materiell-rechtliche Ermächtigung im Kommunalabgabengesetz zum Erlass einer Kommunalen (Steuer-)Satzung beinhaltet nicht ohne weiteres die Befugnis, ohne besondere Ermächtigung des staatlichen Gesetzgebers in die Grundrechte des Bürgers einzugreifen (vgl. wenn auch in anderem Zusammenhang BVerwG NJW 1993, 411). Aus der Befugnis zur Regelung der Einzelheiten eines Steuertatbestandes kann nicht auf die Ermächtigung, auch in das Recht auf informationelle Selbstbestimmung einzugreifen, geschlossen werden. Inhalt, Zweck und Ausmaß der Ermächtigung wären damit aus meiner Sicht überschritten.
- Die alleinige Anwendung des § 93 AO, auf den im Kommunalabgabengesetz verwiesen wird, setzt voraus, dass zur Beteiligung anderer Personen bei der Feststellung eines für die Besteuerung erheblichen Sachverhalts ein konkreter Anlass für das Ersuchen um eine Datenübermittlung zu einer anderen Person gegeben sein muss. Dieser hinreichende Anlass soll vorliegen, wenn aufgrund konkreter Anhaltspunkte oder aufgrund allgemeiner Erfahrung ein Übermittlungsersuchen angezeigt ist. Die Tatsache, dass Steuergesetze nicht immer beachtet werden, soll keine allgemeine Erfahrung in diesem Sinne darstellen (Klein/Orlopp, Kommentar zur AO, 5. Auflage 1995 Anm. 1 zu § 93 AO unter Berufung auf BFH BStBl. 90, 280). Konkrete Anhaltspunkte für steuerlich relevante Sachverhalte lassen sich aus der bloßen Tatsache des Erwerbs eines Hundes aber nicht ableiten.

Nach meiner Auffassung kann die Verpflichtung einer Privatperson aus Anlass eines Kaufvertrages eine andere Person als Erwerber gegenüber einer öffentlichen Stelle benennen zu müssen, nicht durch den Erlass einer kommunalen Satzung begründet werden.

Verdeutlicht wird diese Auffassung besonders dann, wenn der Geltungsbereich des „Ortsrechts“, das durch die Satzung begründet wird, nicht ausreicht und Daten von Hundeerwerbern, die nicht in der Stadt wohnen, gegenüber dem Stadtsteueramt offenbart werden, obwohl sie nicht in dieser Stadt steuerpflichtig werden können.

Leider sind beide Ministerien meiner Auffassung nicht gefolgt und haben sich auf die rein deklaratorische Bedeutung der kommunalen Satzung berufen, die § 93 AO lediglich wiederhole. Dass auch dort vorrangig eine Datenerhebung beim Betroffenen normiert ist, wurde außer Acht gelassen. Feststellbar ist außerdem, dass der Bundesgesetzgeber – so zuletzt aus Anlass des Entwurfs eines Steuervergünstigungsabbaugesetzes – des Öfteren schon betont hat, „Ermittlungen ins Blaue“ hinein, seien nach § 93 AO und der dort festgelegten Subsidiarität der Datenerhebung bei Dritten, nicht zulässig. Zudem fehlt die Transparenz bei der Datenübermittlung, da lediglich Einwohner der jeweiligen Stadt das Ortsrecht kennen müssen.

Aufgrund entsprechender Einlassungen mir gegenüber ist zu befürchten, dass Hundeerwerber ihr Recht auf informationelle Selbstbestimmung gerichtlich geltend machen werden.

7.2 Mitteilungen an die Finanzbehörde

Eine oberste Landesbehörde hat mich um Stellungnahme gebeten, inwieweit personenbezogene Mitteilungen an Finanzbehörden ergehen dürfen, wenn im Rahmen ihrer Kontrolltätigkeit steuerlich relevante Unregelmäßigkeiten aufgedeckt werden.

In erster Linie habe ich empfohlen, gemeinsam mit der Finanzverwaltung Kriterien bezogen auf die Kontrolltätigkeit der anfragenden Behörde festzulegen, die die Steuerstraftat von der Steuerordnungswidrigkeit abgrenzen. Nur für die Steuerstraftat besteht nach § 116 Abgabenordnung eine Anzeigepflicht der Behörden, wenn sie dienstlich Tatsachen erfahren, die den Verdacht einer Steuerstraftat begründen. Aber auch hier ist zu beachten, dass die Wahrung des Brief-, Post- und Fernmeldegeheimnisses gegenüber diesen Anzeigeverpflichtungen vorrangig ist (§ 116 Abs. 2 i.V.m. § 105 Abs. 2 Abgabenordnung).

Übermittlungen an die Finanzbehörden sollten letztendlich nur aufgrund eindeutiger Sachverhalte erfolgen, wobei generalisierende Regelungen bereichsspezifische Übermittlungsverbote aufführen und auch Bagatellgrenzen enthalten sollten.

7.3 Steuernummer auf der Rechnung

Für einigen Wirbel hatte eine neu eingefügte Bestimmung im Umsatzsteuergesetz gesorgt, die durch das Steuerverkürzungsbekämpfungsgesetz eingefügt worden ist.

Unternehmer, die nach dem 30. Juni 2002 Rechnungen ausgestellt haben, wurden gesetzlich verpflichtet, ihre Steuernummer auf den Rechnungen anzugeben. Das damit verbundene Risiko für das Recht auf informationelle Selbstbestimmung wurde von den Medien getestet. Wie den Medienberichten zu entnehmen war, gelang es nur mit Hilfe der Angabe der Steuernummer auf der Rechnung telefonische Auskünfte bei Finanzämtern über Details zu Umsatzsteuervorauszahlungen oder Steuerschulden zu erhalten; nur in einem einzigen Fall sei eine Frage nach der Legitimation des Anrufers gestellt worden.

Da mithin die Steuernummer in der Praxis der Finanzämter wie eine persönliche Geheimnummer (PIN) behandelt wird, ist für Auskunftsersuchen – wie mein hessischer Kollege dies gefordert hat – eine echte PIN zu verlangen, ohne die es keine Auskunft geben darf.

Der Appell an die Finanzbehörden in Form eines Erlasses des Bundesministeriums für Finanzen „bei Zweifeln an der Identität oder Berechtigung eines Auskunftssuchenden müssen sich die Finanzbehörden hierüber in geeigneter Weise vergewissern“, ist offenkundig zur Verhinderung von Missbräuchen nicht ausreichend.

7.4 Finanzamtsübergreifender Zugriff der Zentralen Erbschaft- und Schenkungsteuerstelle

Durch den Jahresbericht 2000 des Rechnungshofes des Saarlandes über die Haushalts- und Wirtschaftsführung des Saarlandes mit Bemerkungen zur Landeshaushaltsrechnung 1999 und Stellungnahme der Landesregierung (Landtagsdrucksache 12/555), erhielt ich erstmals Kenntnis von dem vom Rechnungshof geforderten finanzamtsübergreifenden Zugriff der Zentralen Erbschaft- und Schenkungsteuerstelle auf verschiedene Steuerfestsetzungs- und Steuererhebungsdaten der Finanzämter. Die Forderung wurde damit begründet, dass dadurch eine zügigere Bearbeitung – insbesondere der Erbschaftsteuerfälle - ermöglicht würde und die Steuereinnahmen des Landes besser ausgeschöpft werden könnten. Seitens des zuständigen Ressorts – des Ministeriums für Finanzen und Bundesangelegenheiten – wurde ich über das Vorhaben erstmals im Juni 2002 unterrichtet.

Durch einen uneingeschränkten Zugriff der Erbschaft- und Schenkungsteuerstelle wird diese in die Lage versetzt, Grundinformations-, Festsetzungs- und Erhebungsdaten aus allen Finanzamtsbezirken abzurufen. Dadurch würde dieser Stelle ermöglicht, die Steuerdaten eines jeden erfassten Steuerpflichtigen im Saarland abzurufen. Bei einem Online-Abruf sind die sonst bei Übermittlungen vorhandenen Überprüfungsmöglichkeiten, die sich auf die Zulässigkeit des Abrufs und auf berechtigte Zweifel an der Rechtmäßigkeit beziehen (vgl. § 14 Abs. 3 SDSG), nicht mehr vorhanden, da jeder Sachbearbeiter eigenständig – ohne mündliche Kommunikation mit dem örtlich zuständigen Finanzamt – Daten abrufen kann. Gegenüber einem Ersuchen auf mündliche Übermittlung vervielfältigen sich bei einem Online-Zugriff die Missbrauchsmöglichkeiten, die jeden Sachbearbeiter der Erbschaft- und Schenkungsteuerstelle in die Lage versetzen, völlig allein zu agieren.

Aus diesem Grund sind die gesetzlichen Voraussetzungen, unter denen der automatisierte Abruf von Steuerdaten zulässig ist – insbesondere § 30 Abs. 6 Abgabenordnung (AO) – besonders sorgfältig zu beachten.

Sowohl nach der Bestimmung des § 30 Abs. 6 AO als auch der Regelung einer Verwaltungsvorschrift, die bisher nicht in eine Rechtsverordnung gem. § 30 Abs. 6 AO umgesetzt wurde, ist ein automatisierter Abruf von Steuerdaten nur zulässig soweit der Abruf u.a. der Durchführung eines Verwaltungsverfahrens in Steuersachen dient. Dies ist dann der Fall, wenn wegen des Umfangs der anfallenden Daten, ihrer häufigen oder besonders eilbedürftigen Nutzung unter Berücksichtigung der schutzwürdigen Belange der Betroffenen das Abrufverfahren angemessen ist.

Inwieweit diese Voraussetzungen erfüllt sind, wurde in einer Besprechung mit dem Ministerium für Finanzen und Bundesangelegenheiten 2002 eingehend erörtert. Dabei wurde Einvernehmen darüber erzielt, dass ein genereller unbeschränkter Zugriff der Erbschaft- und Schenkungsteuerstelle auf die Daten der Finanzämter unverhältnismäßig und somit unzulässig ist. Zur Aufgabenerfüllung der vorbezeichneten Dienststelle ist ein temporärer lesender Zugriff auf im Einzelfall festzulegende Grundinformations-, Festsetzungs- und Erhebungsdaten von Betroffenen ausreichend. Die Vollprotokollierung jedes Datenabrufes wird dabei sichergestellt. Die Zugriffe sind jeweils im Einzelnen zu begründen. Mit Hilfe der Sterbefallanzeigen wird eine stichprobenartige Kontrolle der Datenabrufe vorgesehen. Durch die lediglich temporäre Rechtevergabe wird die Zugriffsbeschränkung auf die für die Durchführung des konkreten Besteuerungsverfahrens notwendigen Steuerdaten sichergestellt.

Des Weiteren wird der zentralen Stelle der Zugriff auf die gespeicherten Bewertungsdaten des Landes zu Auskunftszwecken ermöglicht; eine temporäre Rechtevergabe in Einzelfällen ist allerdings im Bewertungsbereich bisher programmtechnisch nicht realisiert. Sie erscheint auch unzweckmäßig, da sich die Belegenheit evtl. vorhandener Grundstücke über mehrere Finanzamtsbezirke erstrecken kann. Allerdings wird eine Vollprotokollierung der Datenabrufe bei Einrichtung des Verfahrens auch für diesen Bereich sichergestellt.

Die ebenfalls in Erwägung gezogene Datenübermittlung aus dem Liegenschaftskataster (DABLIKA) ist nur zulässig, wenn die durch die Änderung des § 29 Abs. 3 Bewertungsgesetz den Finanzbehörden eingeräumte Anordnungsbefugnis ausgefüllt wird. In welcher Form, in welchem Umfang und für welche Fälle dies geschehen darf, wäre noch eingehend zu erörtern.

7.5 Steuervergünstigungsabbaugesetz

Das Bundeskabinett hat am 20.11.2002 den Entwurf des „Gesetzes zum Abbau von Steuervergünstigungen und Ausnahmeregelungen (Steuervergünstigungsabbaugesetz)“ beschlossen.

Da der Entwurf eine sorgfältige Abwägung zwischen der Steuergerechtigkeit und dem informationellen Selbstbestimmungsrecht vermissen lässt, haben die Datenschutzbeauftragten des Bundes und der Länder in einer gemeinsamen Stellungnahme ihre Bedenken gegen den Entwurf geäußert. Dabei haben sie insbesondere auf die Aufhebung des § 30a Abgabenordnung – und somit den Wegfall des Bankgeheimnisses – sowie die erweiterten Meldepflichten der Banken und anderer Finanzdienstleister mit Hilfe eines neuen einheitlichen Identifikationsmerkmales hingewiesen. Die Einzelheiten der gemeinsamen Stellungnahme ergeben sich aus Anlage 9.

8 Meldewesen

8.1 Melderegisterauskunft bei Namensgleichheit

Fälle, in denen Bürgern Unannehmlichkeiten dadurch erwachsen, dass sie durch Auskünfte öffentlicher Stellen – insbesondere im Rahmen der Melderegisterauskunft – mit Personen gleichen Namens verwechselt werden, kommen – wie dies Eingaben belegen – in der Praxis immer wieder vor. Der vorliegende Fall unterscheidet sich jedoch dadurch, dass dem Betroffenen wegen falscher Auskünfte in der Vergangenheit sowie aufgrund weiterer Umstände eine Auskunftssperre gemäß § 34 Abs. 5 Saarländisches Meldegesetz wegen Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange von der Gemeinde zugebilligt wurde. Die Gemeinde teilte dem Betroffenen dies schriftlich mit und hat nach eigener Aussage auch eine entsprechende Sperre Mitte 2001 im Melderegister eingetragen. Im September 2002 musste der betroffene Bürger jedoch feststellen, dass offensichtlich keinerlei Sperre (mehr) eingetragen war und somit – trotz Weiterbestehens der dargestellten Gefahr – jedermann Auskunft aus dem Melderegister bekommen konnte.

Bei meiner Überprüfung im Meldeamt bestätigte sich dieser Sachverhalt. Eine Erklärung dafür, wie dies möglich war, konnte von der Gemeinde nicht gegeben werden. Insbesondere ließ sich nicht feststellen, ob die Sperre eingetragen war oder versehentlich gelöscht wurde, da eine eventuelle Protokollierung bisher nicht vorgelegt wurde. Allerdings zeigte die Überprüfung auch, dass das Einrichten der Auskunftssperre und insbesondere die Löschung durch jeden Mitarbeiter der Meldebehörde möglich war und keinerlei Beschränkung unterlag.

Die Aufhebung von Auskunftssperren nach § 34 Abs. 5 Saarländisches Meldegesetz wegen Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnlicher schutzwürdiger Belange durch jeden Mitarbeiter halte ich wegen der für den Betroffenen eventuell weiter bestehenden Gefahren nicht für sachgerecht. Die Löschung müsste entweder einzelnen Mitarbeitern übertragen sein oder es müsste zumindest eine automatisiert unterstützte Überprüfung erfolgen, damit die Gefahren für den Betroffenen durch die automatisierte Melderegisterführung auf ein Mindestmaß reduziert werden.

Darüber hinaus habe ich vorgeschlagen, um weiteren Verwechslungen bei Namensgleichheit besser begegnen zu können, dem Betroffenen ein Dokument auszustellen, in dem ihm bestätigt wird, dass er nicht die Person ist, mit der er verwechselt wird. Diese Maßnahme wird im Polizeibereich bei Verwechslungsgefahr im Zusammenhang mit der Ausschreibung zur Fahndung ebenfalls angewandt.

Eine abschließende Stellungnahme der Gemeinde steht noch aus.

8.2 Veröffentlichung der Daten von Alters- und Ehejubilaren

Aufgrund von Eingaben Betroffener, die Unverständnis darüber äußerten, dass ihre Daten bei Alters- oder Ehejubiläen an die Presse übermittelt wurden, die ihrerseits dieses Daten veröffentlichte, hat sich die Frage gestellt, ob die entsprechende Rechtsgrundlage im Meldegesetz und deren Auslegung insbesondere auch im Lichte der EU-Datenschutzrichtlinie noch verfassungsrechtlichen Anforderungen genügt. Die Petenten fühlten sich durch die Veröffentlichung ihres Alters (ab 70. Lebensjahr) oder des Alters ihrer Ehe (ab Goldener Hochzeit) in ihrem Recht auf informationelle Selbstbestimmung verletzt. Keinem war es bewusst, dass solche Veröffentlichungen durch einen Widerspruch gegen die Herausgabe der Daten hätte vermieden werden können.

Die Rechtsgrundlage im saarländischen Meldegesetz kann keineswegs als normenklar angesehen werden. Hinzu kommt eine Auslegungspraxis, die über den Wortlaut der Bestimmung hinausgeht und zur Intransparenz behördlichen Handelns beiträgt.

Der Wortlaut der Rechtsgrundlage findet sich in § 35 Abs. 2 des Saarländischen Meldegesetzes in der ursprünglichen Fassung aus dem Jahr 1982. Dort heißt es schlicht, wenn jemand eine Melderegisterauskunft über Alters- oder Ehejubiläen von Einwohnern begehrt, so darf ihm diese Auskunft erteilt werden, sofern der Betroffene nicht widersprochen hat. Auf das Widerspruchsrecht ist mindest einmal im Jahr durch öffentliche Bekanntmachung hinzuweisen.

Aus dem Wortlaut kann das, was danach in den Kommunen abläuft, nicht herausgelesen werden. Zum einen dürfte die Presse nicht alle Daten von Personen gruppenweise erhalten, die keinen Widerspruch eingelegt haben. Der Gesetzgeber hat diese Absicht, Gruppenauskünfte u.a. an die Presse als zulässig zu erachten, nicht klar und für jeden Bürger verständlich festgelegt. Zum andern enthält die Norm nicht die Zweckbestimmung, dass die Daten veröffentlicht werden dürfen. Eine Veröffentlichung, die sich stets an eine unbestimmte Personenanzahl richtet, beinhaltet eine verstärkte Qualität des Eingriffs in das Recht auf informationelle Selbstbestimmung und bedarf daher eines Wortlautes, der die beabsichtigte Veröffentlichung im Gesetzestext offen legt.

Ich sehe daher auf der Grundlage dieses Wortlauts allenfalls eine (Einzel-) Auskunft an Private für zulässig an, denen es in erster Linie um eine persönliche Gratulation geht und nicht um eine Veröffentlichung dieser Daten durch Presseorgane, mit allen unliebsamen Folgen, die die Veröffentlichung für Jubilare mit sich bringen kann.

Wie ein Petent berichtete, hatte die für ihn gänzlich überraschende Veröffentlichung im Gemeindeblatt und zusätzlich einer überregionalen Zeitschrift Gratulationen aus Anlass seines 70. Geburtstags zur Folge, die sich über Wochen hinzogen. Hinzu kamen noch verstärkte anlassbezogene Werbeversuche durch die Auswertung der Presse, die wohl regelmäßig durch Wirtschaftsunternehmen vorgenommen werden.

Nach heutigem Datenschutzverständnis sollten öffentliche Stellen Datenübermittlungen aufgrund einer Widerspruchslösung nicht vornehmen dürfen, da die Beschwerdeführer zu Recht einwenden, ihre Einwilligung werde aufgrund irgendwelcher Presseveröffentlichungen zum Widerspruchsrecht letztlich doch nur fingiert.

Dem Gesetzgeber möchte ich empfehlen, die Bestimmung, wie dies in anderen Bundesländern schon geschehen ist, dem neuzeitlichen Verständnis von Datenschutz anzupassen und demzufolge für die Auskunftserteilung die Einwilligung des Betroffenen vorzusehen (s. § 35 Abs. 2 Hamburgisches Meldegesetz; § 35 Abs. 3 Meldegesetz Nordrhein-Westfalen). Die Problematik ist im Übrigen vergleichbar mit der im Jahr 1997 datenschutzfreundlich novellierten Auskunft an Adressbuchverlage, der seither ebenfalls eine Einwilligung zugrunde liegen muss.

Inwieweit in der kommunalen Praxis Datenübermittlungen zur Vornahme von Ehrungen bei Alters- und Ehejubiläen innerhalb des öffentlichen Bereichs erfolgen sollen, für den es eine eigenständige Rechtsgrundlage gibt (§ 33 Abs. 2 Meldegesetz), wäre bei dieser Gelegenheit ebenfalls zu überdenken.

Auch hier verbietet sich aufgrund der gleichen Überlegungen, wie dargestellt, eine eigene Veröffentlichung durch die Gemeinde, da die Intensität des Eingriffs in das Recht auf informationelle Selbstbestimmung die gleichen Auswirkungen zur Folge hat, unabhängig davon, welche Stelle die Veröffentlichung veranlasst.

8.3 Veröffentlichungen der Namen von Vereinsmitgliedern im amtlichen kommunalen Bekanntmachungsblatt

Eine Vielzahl von Bürgern und Bürgerinnen hatte sich zu Recht darüber beschwert, dass ihre Namen als Mitglieder eines religiös orientierten Vereins sowie ihre vollständigen Adressen im Gemeindeblatt veröffentlicht worden sind. Dies geschah im Zusammenhang mit der Einladung zu einer Mitgliederversammlung, an der auch der Bürgermeister teilnehmen sollte.

Die Erforderlichkeit für die Veröffentlichung, die über die Datenangaben hinaus Aufschluss der Vereinsmitglieder über ihre religiöse Ausrichtung gab, war nicht zu begründen. Auch für den Hauptausschuss der Gemeinde, dem diese personenbezogene Unterlage ebenfalls vorgelegen hat, ergab sich keine Notwendigkeit anhand dieser Daten, eine Erörterung der Thematik vorzunehmen.

Ich habe den Bürgermeister der Gemeinde darauf hingewiesen, dass eine unzulässige Datenübermittlung an die Öffentlichkeit stattgefunden hat und zudem der Grundsatz der Datensparsamkeit nicht beachtet wurde. Im Zusammenhang mit dem Inhalt einer religiösen Überzeugung ist die Prangerwirkung durch Veröffentlichungen unverkennbar.

Auch hier wurde der zentrale Gesichtspunkt der Erforderlichkeit eines Personenbezugs wiederum vernachlässigt (s.a. 18. TB, TZ 8.1; 17. TB, TZ 6.2).

8.4 Melderechtsrahmengesetz

Die elektronische Datenverarbeitung hat auch verstärkt Einzug in das Melderecht gehalten.

Zur Änderung des Melderechtsrahmengesetzes haben die Datenschutzbeauftragten des Bundes und der Länder im Zuge des Gesetzgebungsverfahrens in einer Entschließung Stellung bezogen (Anlage 10). So wurde zwar grundsätzlich die Absicht begrüßt, mit Blick auf die neuen Informations- und Kommunikationstechnologien das Meldewesen zu modernisieren. Nicht in Vergessenheit geraten dürfen dabei aber die schützwürdigen Belange Betroffener, insbesondere bei der (einfachen) Melderegisterauskunft an Dritte, bei der die Schnelligkeit der Auskunftserteilung nicht zu einem Risiko im Hinblick auf die Richtigkeit und Gefahrlosigkeit der Auskunft geraten darf. Von Bedeutung ist insofern, dass der Betroffene einem automatisierten Abruf seiner Daten über das Internet widersprechen kann und damit einem Anliegen der Datenschutzbeauftragten Rechnung getragen wurde.

Zu weiteren in der Entschließung enthaltenen Forderungen ist nunmehr ein Appell an den Landesgesetzgeber zu richten, der die Umsetzung des Melderechtsrahmengesetzes in das Landesrecht vorzunehmen hat, da datenschutzfreundlichere Gestaltungen des Landesmelderechts in einigen Punkten durchaus zulässig wären.

Ein Änderungsentwurf zum saarländischen Meldegesetz ist mir bisher allerdings nicht bekannt.

9 Wahlen und Einwohnerbefragungen

9.1 Repräsentative Wahlstatistik und das Wahlgeheimnis

Bedauerlicherweise sind sowohl der Bundes- als auch der Landesgesetzgeber bislang den Aufforderungen, die repräsentative Wahlstatistik entfallen zu lassen, nicht gefolgt.

Nach der Bundestagswahl 2002 habe ich die Durchführung der Wahlstatistik beim Statistischen Amt des Landes überprüft. Dabei habe ich besonderes Augenmerk auf die bei der Wahlstatistik bekannten Problempunkte gelegt (s. 15. TB, TZ 6.1). So wurde festgestellt, dass einzelne Gemeinden es versäumt hatten, entgegen der gesetzlichen Anordnung, die verpackten Stimmzettel vor dem Versand an das Statistische Amt zu versiegeln.

Eine der herausragenden Schwachstellen für eine Durchbrechung des Wahlgeheimnisses ist die Auszählung der für die repräsentative Wahlstatistik ausdrücklich gekennzeichneten Stimmzettel hinsichtlich des Wahlverhaltens. Statistische Ergebnisse werden sowohl zur Wahlbeteiligung als auch zur einzelnen Stimmabgabe (Wahlverhalten) ermittelt. Die Tatsache der bloßen Nichtbeteiligung an der Wahl ist zwar weniger eingriffsintensiv als das Votum einer bestimmten Person für einen bestimmten Wahlvorschlag, wenngleich auch die Nichtbeteiligung als politisches Votum verstanden werden kann und schon aus diesem Grunde der Geheimhaltung bedarf.

Findet eine Wahlbeteiligung statt, so kann, aufgrund der statistischen Kennzeichnung der Stimmzettel nach Geschlecht und Geburtsjahresgruppen, das Votum im Stimmzettel an Hand des Wählerverzeichnisses unter bestimmten Voraussetzungen einer konkreten Person zugeordnet werden.

Bei der Auswertung der Stimmabgabe ist nach dem Wahlstatistikgesetz des Bundes daher eine Zusammenführung von gekennzeichneten Stimmzetteln und Wählerverzeichnissen unzulässig. Dieser gesetzlichen Vorgabe, die das Wahlgeheimnis sichern soll, muss in der Durchführung der Wahlstatistik Rechnung getragen werden, damit die Wahlentscheidung geheim bleibt.

Es sollte daher als eine herausragende Pflicht für jede Wahlleitung angesehen werden, das gesetzliche Verbot der Zusammenführung von Wählerverzeichnissen und Stimmzetteln durch bestmögliche organisatorische Maßnahmen sicherzustellen.

Das Ministerium für Inneres und Sport habe ich gebeten, für die Landeswahlen ein entsprechendes gesetzliches Verbot in die Wege zu leiten.

Meine Präferenz, auf die Durchführung repräsentativer Wahlstatistiken gänzlich zu verzichten, habe ich bei dieser Gelegenheit wiederum betont. Die Gründe für diesen Vorschlag scheinen mir augenfällig zu sein. Angesichts der heutigen Möglichkeiten, das Wählerverhalten durch private Institute zu erforschen, ist es keineswegs zweifelsfrei, ob die mit der Durchführung der Wahlstatistiken verbundenen Gefahren für das Recht auf informationelle Selbstbestimmung im überwiegenden Interesse der Allgemeinheit hinzunehmen sind (Art. 2 SVerf).

9.2 Einhaltung von Wahlrechtsgrundsätzen

Nach einer Bürgermeisterwahl wurden Beschwerden an mich herangetragen, weil in der Gemeinde bekannt geworden sein sollte, wer eine Unterstützungsliste für einen freien Bürgermeisterkandidaten unterzeichnet hatte. Zunächst war zu klären, ob Unbefugte in die Unterstützungsliste Einblick nehmen konnten. Dies war jedoch nicht feststellbar.

Aus der Tatsache, dass Personen an einem der Samstagvormittage, an denen das Rathaus nach Kommunalwahlrecht zur Unterschriftsleistung offen zu halten war, dort anwesend waren, haben Bedienstete der Kommune gefolgert, dies könne nur zwecks Unterschriftsleistung der Fall gewesen sein. Die Vermutung wurde an die Presse und insbesondere an die politische Partei weitergegeben, die darin einen Anlass zur Einleitung von Parteiausschlussverfahren ihrer angeblich betroffenen Mitglieder gesehen hat, denn sowohl der freie Kandidat als auch ein Gegenkandidat waren zum Zeitpunkt der Wahl Mitglieder derselben politischen Partei. Der freie Kandidat hatte allerdings nicht die Unterstützung seiner Partei.

Ich habe wegen der gravierenden Missachtung von Wahlrechtsgrundsätzen, hier vor allem des Wahlgeheimnisses, die Angelegenheit förmlich beanstandet. Obwohl eine Einsichtnahme durch Unbefugte in die Unterstützungsliste nicht festgestellt werden konnte, hatte die Weitergabe der Beobachtung von Bediensteten, welche Personen an einem Samstagvormittag das Rathaus betreten haben, die gleichen Auswirkungen wie ein Einblick in die Unterstützungsliste. Die danach in die Wege geleiteten Parteiausschlussverfahren belegen dies in eindrucksvoller Weise.

Damit Unterschriftsleistenden auch bei diesem Vorgang eine geheime Wahl gewährleistet wird, hat der Verordnungsgeber in der Kommunalwahlordnung für jeden Unterschriftsleistenden ein eigenes Unterschriftsblatt vorgesehen, so dass eine Kenntnisnahme bei Gelegenheit der Unterschriftsleistung von anderen Unterstützern eines Wahlvorschlags ausgeschlossen werden kann. Er hat außerdem festgelegt, welche Personen befugt sind, in die Unterstützungsliste Einblick zu nehmen.

Die Bestimmungen dienen bereits im Vorfeld der Wahl dem Schutz des Rechts auf informationelle Selbstbestimmung, denn die Unterstützer eines Wahlvorschlags sind im Rahmen ihrer Unterschriftsleistung in gesteigertem Maße auf die Verschwiegenheit der Bediensteten der Gemeindeverwaltung angewiesen, zumal sie ihre Identität als Wahlberechtigte namentlich nachzuweisen haben. Zudem spricht ein erhöhter Grad der Wahrscheinlichkeit dafür, dass der unterstützte Kandidat auch später die Stimme des Unterschriftsleistenden erhalten werde, so dass insofern auch der Kerninhalt des Wahlgeheimnisses berührt ist.

Diese Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung, das vorliegend im Wahlgeheimnis seinen Ausdruck findet, werden in gravierendem Maße unterlaufen, wenn Bedienstete Tatsachen – wie das Erscheinen an einem Samstagvormittag im Rathaus – nach außen tragen, die den Schluss auf eine Unterschriftsleistung für einen Wahlvorschlag nahe legen können. Gerade weil diese Schlussfolgerung nicht zwingend ist und auch andere Gründe für einen Aufenthalt im Rathaus an einem Samstagvormittag vorstellbar sind, ist diese dienstliche Wahrnehmung besonders schützenswert und darf von Seiten der mit diesem Teil des Wahlvorgangs befassten Bediensteten nicht an Unbefugte sowohl innerhalb als auch außerhalb der Gemeindeverwaltung übermittelt werden.

Die Erforderlichkeit und damit die Zulässigkeit einer Übermittlung innerhalb des öffentlichen Bereichs gem. § 14 Saarländisches Datenschutzgesetz, aber erst recht die Zulässigkeit einer Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs gem. § 16 Saarländisches Datenschutzgesetz war demnach nicht gegeben.

Ich habe außerdem darauf hingewiesen, dass die Auswirkungen des Datenschutzverstoßes nicht weiter Platz greifen dürfen, so dass die Datenempfänger einem Verwertungsverbot im Hinblick auf die verbreiteten Tatsachen und Schlussfolgerungen unterliegen.

Das Ergebnis meiner rechtlichen Bewertung ergibt sich im Übrigen auch aus dem allgemeinen Grundsatz der Amtsverschwiegenheit, der eine Weitergabe dienstlicher Wahrnehmungen selbstverständlich ebenfalls verbietet.

9.3 Datenschutzgerechte Durchführung einer Einwohnerbefragung

Nach dem Kommunalselbstverwaltungsgesetz (§ 20b) können die Einwohner und Einwohnerinnen zu wichtigen Angelegenheiten der Gemeinde aufgrund eines Gemeinderatsbeschlusses befragt werden. Das Nähere dazu ist im Wege einer kommunalen Satzung zu beschließen.

Gemeinden, die eine Einwohnerbefragung durchführen wollten, haben entsprechende Satzungen erlassen.

Im Kommunalselbstverwaltungsgesetz ist vor allem die datenschutzrechtlich bedeutsame Bestimmung enthalten, dass eine Befragung in anonymisierter Form zu erfolgen hat. Insbesondere dieses Gebot ist in der Satzung zu konkretisieren. Im Gesetz selbst ist auch die Freiwilligkeit der Teilnahme an der Einwohnerbefragung festgelegt.

Der Datenschutzbeauftragte einer Gemeinde sah das Anonymisierungsgebot durch eine Satzungsbestimmung nicht ausreichend gewahrt, die wie folgt lautete:

> „In dem Verzeichnis der teilnahmeberechtigten Einwohnerinnen und Einwohner wird auch vermerkt, wer seine Stimme abgegeben hat."

Da die Einwohnerbefragung der bei allgemeinen Wahlen geltenden Grundsätze der Urnen- und Briefwahl nachgebildet sein sollte, erschien diese Regelung auf den ersten Blick unproblematisch. Das Ministerium für Inneres und Sport hat die Anonymisierung durch die Geheimhaltung des Inhalts der Stimmabgabe auch für ausreichend angesehen. In den Wählerverzeichnissen wird die Teilnahme an allgemeinen Wahlen ebenfalls vermerkt.

In meiner Stellungnahme, um die ich gebeten wurde, habe ich jedoch die Frage gestellt, ob Ziel und Zweck einer Einwohnerbefragung nicht auch in verstärkter Anonymität zu erreichen seien, so dass entsprechend dem Prinzip der Datenvermeidung und Datensparsamkeit (§ 4 Abs. 4 SDSG) dieser Weg zu wählen wäre.

Um verfassungsrechtlichen Anforderungen Genüge zu tun, müssten Datenverarbeitungsschritte auf das zur Zweckerreichung absolut notwendige Maß beschränkt werden.

Dazu könnte folgendes – ebenso erfolgversprechendes wie darüber hinaus kostenreduzierendes – Verfahren in Betracht kommen:

Jedem Berechtigten, der anhand des Melderegisters ermittelt wird, ist ein amtlicher Vordruck zu übersenden. Der Rücklauf der amtlichen Vordrucke wäre nicht zu registrieren, wenn durch (nicht personenbeziehbaren) Zahlenaufdruck sichergestellt würde, dass nur amtliche Vordrucke gezählt werden. Ein Teilnehmerverzeichnis wäre demnach nur für die Versendung der amtlichen Vordrucke erforderlich, es wäre danach unverzüglich zu vernichten.

Damit würde letztlich erreicht, dass die Teilnahme an der Einwohnerbefragung innerhalb der Behörde nicht durch Abgleich mit dem Teilnehmerverzeichnis bekannt wird.

Von Seiten des Ministeriums für Inneres und Sport wurde für eine Neuberatung der Satzungsvorschriften empfohlen – auch unter dem Gesichtspunkt einer etwaigen Kostenreduzierung –, diese Überlegungen mit einzubeziehen.

10 Soziales

10.1 Datenabgleich beim BAföG mit dem Bundesamt für Finanzen

Von Kollegen habe ich erfahren, dass in anderen Bundesländern ein Datenabgleichverfahren zwischen den BAföG-Ämtern und dem Bundesamt für Finanzen stattfindet, um die Vermögensangaben von BAföG-Antragstellern zu überprüfen. Das Bundesamt für Finanzen kennt die Höhe der in Anspruch genommenen Freistellungsbeträge. Aus den vom Bundesamt für Finanzen den BAföG-Ämtern mitgeteilten Zinseinkünften lassen sich Rückschlüsse auf das Vermögen des Auszubildenden ziehen. Die BAföG-Ämter können vergleichen, ob das im Antrag angegebene Vermögen dem aufgrund der Zinseinnahmen vermuteten Vermögen entspricht und gegebenenfalls Rückforderungsbescheide erlassen.

Meine Nachfrage bei dem zuständigen Ministerium für Bildung, Kultur und Wissenschaft hat ergeben, dass im Saarland dieser Datenabgleich bisher noch nicht durchgeführt wird. Ich habe das Ministerium gebeten, von dem Abgleichverfahren vorerst Abstand zu nehmen. Denn auch wenn es zutreffend sein mag, dass auf diesem Wege eine Fülle unehrlicher Antragsteller ausfindig gemacht werden kann, so ist für mich keine Rechtsgrundlage ersichtlich, die den Datenaustausch legitimieren könnte.

In § 45 d Abs. 2 Einkommensteuergesetz ist zwar vorgesehen, dass das Bundesamt für Finanzen den Sozialleistungsträgern bestimmte Daten mitteilen darf, soweit dies zur Überprüfung des bei der Sozialleistung zu berücksichtigenden Einkommens oder Vermögens erforderlich ist.

Eine entsprechende Befugnisnorm für die Übermittlung von Sozialdaten von den BAföG-Ämtern an das Bundesamt für Finanzen fehlt jedoch. Nach der eindeutigen Vorschrift des § 67 d SGB X ist eine Übermittlung von Sozialdaten nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X oder nach einer anderen Rechtsvorschrift des SGB vorliegt. Eine solche die Datenübermittlung legitimierende Rechtsvorschrift kann ich nicht erkennen. § 45 d EStG vermag diese fehlende Rechtsgrundlage nicht zu ersetzen. Weder handelt es sich bei dieser Vorschrift um eine solche des SGB noch enthält sie eine Regelung zur Übermittlung von Sozialdaten der Ämter für Ausbildungsförderung an das Bundesamt für Finanzen.

Vor Schaffung einer entsprechenden Rechtsgrundlage darf deshalb mit dem Abgleichverfahren nicht begonnen werden.

Ob das Ministerium meinen Bedenken Rechnung tragen wird, war mir bei Redaktionsschluss nicht bekannt.

10.2 Klientendatei beim Jugendamt

Bei dem Bezirkssozialdienst eines Kreisjugendamtes wurde als Ersatz für die bisherige manuelle Kartei ein PC-Programm eingeführt, mit dem Falldaten der betreuten Kinder/Jugendlichen und ihrer Eltern sowie Bearbeitungshinweise erfasst werden. Ein Sozialarbeiter hatte sich an mich gewandt, weil er wegen der geplanten Auswertungen des Datenbestandes und des großen, zugriffsberechtigten Personenkreises eine Verletzung des Sozialdatenschutzes und eine Beeinträchtigung der ihm nach § 203 Abs. 1 StGB obliegenden Geheimhaltungspflicht befürchtete.

Mit dem Landkreis konnte ich schließlich Einvernehmen über die folgenden datenschutzrechtlichen Anforderungen erzielen:

- Nach § 65 SGB VIII unterliegen Sozialdaten, die dem Jugendamtsmitarbeiter zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden sind, einem besonderen Vertrauensschutz. Diese Angaben dürfen auch innerhalb des Jugendamtes nur unter den im Gesetz im einzelnen genannten Voraussetzungen weitergegeben werden. In der Erfassungsmaske des PC-Programms wird ein Hinweis aufgenommen, dass solche Daten nicht gespeichert werden dürfen.

- Zugriffsberechtigt auf personenbezogene Daten sind wegen des sensiblen Charakters der Angaben nur der jeweils zuständige Sozialarbeiter, sein Vertreter sowie der jeweilige Sachgebietsleiter. Amtsleiter und Sekretariat erhalten keine Zugriffsberechtigung.

- Für Zwecke der Sozial- und Jugendhilfeplanung wird – soweit benötigt - ein anonymisierter Datenbestand gebildet (§ 64 SGB VIII).

10.3 Datenaustausch zwischen den Gemeinden und dem örtlichen Träger der Sozialhilfe

Leistungsträger für die Sozialhilfe sind der Stadtverband und die Landkreise. Diese örtlichen Träger der Sozialhilfe haben die Durchführung der Hilfegewährung weitgehend den Städten und Gemeinden übertragen (§ 4 des saarländischen Ausführungsgesetzes zum Bundessozialhilfegesetz; AG-BSHG). Welche Aufgaben im Einzelnen den Städten und Gemeinden obliegen, haben die Sozialhilfeträger in unterschiedlicher Weise durch Satzung geregelt.

Eine kreisangehörige Stadt bat um datenschutzrechtliche Beurteilung der Datenflüsse zwischen dem örtlichen Sozialamt und dem Kreissozialamt. Der Landkreis hatte ein neues automatisiertes Sozialhilfeprogramm eingeführt und dabei verlangt, dass die Daten aller Sozialhilfeempfänger dem Kreissozialamt übertragen und täglich aktualisiert werden. Das Kreissozialamt erhielt dadurch erstmals einen unmittelbaren Zugriff auf den kompletten Sozialhilfeempfänger-Datenbestand der örtlichen Sozialämter. Die Stadt argumentierte, dass die Gemeinden nach der Delegationssatzung grundsätzlich selbständig zu entscheiden hätten, der Kreis dagegen sich im wesentlichen nur vorbehalten habe, in Einzelfällen und bei bestimmten Hilfearten tätig zu werden.

Nach meiner Auffassung sind die Sozialämter der Gemeinden "verantwortliche Stellen" im datenschutzrechtlichen Sinne (§ 67 Abs. 9 SGB X) und nicht etwa lediglich "Außenstellen der Kreissozialämter". Daraus folgt, dass die Weitergabe von Sozialdaten durch die Sozialämter an den Kreis eine Datenübermittlung darstellt, die einer gesetzlichen Übermittlungsbefugnis bedarf. Eine solche Übermittlungsbefugnis ist in § 69 Abs. 1 Nr. 1 SGB X zu sehen, wenn der Datentransfer zur Erfüllung der Aufgaben der beteiligten Sozialämter erforderlich ist. Das Sozialministerium geht in seiner Stellungnahme davon aus, dass der Landkreis auch bei Heranziehung der Gemeinden weiterhin sachlich zuständig und verantwortlich bleibt, die Durchführung der Aufgaben durch die Gemeinden jederzeit und umfassend zu prüfen sowie generelle als auch Weisungen im Einzelfall zu erteilen. Der Landkreis hat darüber hinaus darauf verwiesen, dass aufgrund der Satzungsregelung das Kreissozialamt bei der Heranziehung Unterhaltspflichtiger deren Leistungsfähigkeit zu prüfen und Unterhaltsbeiträge festzusetzen hat. Des Weiteren würde das Kreissozialamt die laufenden Fälle unter Einbeziehung der Datenlage beim örtlichen Sozialamt in periodischen Abständen überprüfen und – etwa bei einer Regelsatzerhöhung – der aktuellen Rechtslage anpassen. Der Datentransfer vom örtlichen Sozialamt zum Kreissozialamt ist daher als rechtmäßig anzusehen. Das Kreissozialamt muss allerdings dafür sorgen, dass nicht alle Sachbearbeiter uneingeschränkt Zugriff auf den Datenbestand erhalten, sondern jeder Mitarbeiter nur soweit dies für seine Aufgabenerfüllung erforderlich ist. Außerdem sollte der Landkreis seine Delegationssatzung an die geänderte Situation anpassen (automatisierte, zentrale Sozialhilfedatei statt Vorlage der Vorgänge in Papierform).

10.4 Abrechnung von Krankenhilfeleistungen für Sozialhilfeempfänger durch eine Privatfirma

Sozialhilfeempfänger, die nicht krankenversichert sind, haben einen Anspruch auf Krankenhilfe (u.a. ärztliche und zahnärztliche Behandlung, Versorgung mit Arzneimitteln, Verbandsmitteln und Zahnersatz, Krankenhausbehandlung) gegenüber den Trägern der Sozialhilfe. Die Abrechnung dieser Leistungen erfolgte bisher durch die Sozialämter.

Im Berichtszeitraum haben mich mehrere Sozialhilfeträger von ihrer Absicht informiert, die Abrechnung der Krankenhilfeleistungen auf eine private Firma mit Sitz in Essen zu vergeben.

Die Sozialhilfeträger haben mir die entsprechenden Vertragsentwürfe mit der Bitte um eine datenschutzrechtliche Bewertung vorgelegt.

Aufgabe der beauftragten Firma soll u.a. die Prüfung sein, ob die Personen, für die Leistungen in Rechnung gestellt worden sind, dem Grunde nach berechtigt sind, Krankenhilfe zu erhalten. Zu diesem Zweck liefern die Sozialämter der Auftragnehmerin eine Datei der anspruchsberechtigten Krankenhilfeempfänger. Nach Prüfung der Abrechnung auf rechnerische Richtigkeit, Vollständigkeit und Einhaltung der gesetzlichen und vertraglichen Regelungen der Rechnungslegung werden die Rechnungen von der Auftragnehmerin gegenüber den Leistungserbringern zahlbar gestellt.

Bei der geschilderten Konstellation kommt es zu einer Weitergabe von Sozialdaten von der für die Aufgabenerfüllung zuständigen Stelle an einen Dritten. Datenschutzrechtlich war die Frage zu klären, ob hier noch von einer nach § 80 SGB X zulässigen Auftragsdatenverarbeitung auszugehen war oder ob eine darüber hinausgehende Funktionsübertragung stattfinden würde.

Von einer Auftragsdatenverarbeitung ist dann auszugehen, wenn der Gestaltungsrahmen des Auftragnehmers so eng gezogen ist, dass der Verbleib der Verantwortung für die Sachbearbeitung bei dem Auftraggeber hinreichend klar geregelt bleibt. Folgende Gesichtspunkte sprechen für eine Datenverarbeitung im Auftrag:

- Der Auftragnehmer darf keine Entscheidungen fällen, die die Ausübung eines Ermessens oder die Ausfüllung eines Beurteilungsspielraumes verlangen.
- Der Leistungserbringer muss auf Gegenvorstellungen, die er beim Auftraggeber gegen die Ablehnung seiner Rechnung vorbringt, von diesem nach eigener Prüfung eine Antwort erhalten.
- Der Auftragnehmer darf keinen Verwaltungsakt erlassen.
- Der Leistungserbringer muss gegen eine ablehnende Entscheidung Widerspruch beim Auftraggeber einlegen können.

Nach Durchsicht der mir zur Verfügung gestellten Unterlagen bin ich zum Ergebnis gekommen, dass es sich bei der Tätigkeit der privaten Firma überwiegend um Routinetätigkeiten handelt, die keine Ermessensentscheidungen erfordern und anhand festgelegter Kriterien erledigt werden können.

§ 80 Abs. 5 SGB X macht die Zulässigkeit einer Auftragsdatenverarbeitung von Sozialdaten durch nicht-öffentliche Stellen davon abhängig, dass die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst. Ich habe auch diese Zulässigkeitsvoraussetzungen als erfüllt angesehen, so dass ich im Ergebnis, nachdem noch einige Verbesserungsvorschläge in technisch-organisatorischer Sicht umgesetzt worden waren, keine grundsätzlichen Einwände gegen die Auftragserteilung geltend gemacht habe.

10.5 Unzulässige Datenübermittlungen eines Sozialamtes

Die Mitarbeiterinnen und Mitarbeiter beim Sozialamt haben es bei der Gewährung von Sozialhilfe häufig mit psychisch und geistig Kranken zu tun, deren Betreuung manchmal mit besonderen Schwierigkeiten verbunden ist. Dennoch darf das Sozialamt nicht einfach über den Kopf der Betroffenen hinweg handeln; die gesetzlichen Regelungen über den Sozialdatenschutz sind einzuhalten.

Ein Hilfeempfänger hatte sich bei mir beschwert, das Sozialamt habe ihm nicht ordnungsgemäß Auskunft über die gespeicherten Daten erteilt und gebe ohne sein Wissen unzutreffende Informationen an andere Stellen weiter. Da ich aus der Darlegung des Petenten kein klares Bild gewinnen konnte, habe ich die Sozialhilfeakte eingesehen. Dabei musste ich folgendes feststellen:

- Das Sozialamt hatte sich bei der Antragstellung eine „Einwilligungserklärung“ von dem Hilfesuchenden unterzeichnen lassen. Darin werden alle für eine Übermittlung theoretisch in Betracht kommenden Stellen im Einzelnen aufgeführt sowie zusätzlich noch zur Sicherheit: „und andere Behörden“. Solche pauschalen Erklärungen „auf Vorrat“ können jedoch keine Rechtsgrundlage für alle im Laufe der Hilfegewährung anfallenden Datenübermittlungen sein. Eine Einwilligungserklärung darf nur für eine tatsächlich vorgesehene Datenübermittlung verlangt werden, wobei der Hilfeempfänger über den Datenempfänger und den Zweck der Übermittlung zu informieren ist (§ 67b Abs. 2 SGB X).

- Dem Landeskriminalamt wurde auf Aufforderung ein von der Klinik für Forensische Psychiatrie vor 3 Jahren erstellter „Sozialmedizinischer Bericht“ zur Verfügung gestellt. In der Sozialhilfeakte ist nicht dokumentiert, ob die Zulässigkeit dieser Datenübermittlung überprüft und auf welcher Rechtsgrundlage der Bericht schließlich übersandt wurde. Die in § 73 SGB X geregelten Zulässigkeitsvoraussetzungen einer Datenübermittlung für die Durchführung eines Strafverfahrens waren nicht erfüllt. Das Sozialamt hätte besser das LKA an die Klinik, die das Gutachten ausgestellt hat, verwiesen anstatt der ärztlichen Schweigepflicht und dem Sozialgeheimnis unterliegende Unterlagen herauszugeben.

- Mehrere Unterlagen „über den Gesundheitszustand“ des Hilfeempfängers, u.a. der erwähnte sozialmedizinische Bericht sowie mehrere Arbeitsunfähigkeitsbescheinigungen mit Diagnoseangaben, wurden dem Landkreis (Amt für Arbeitsförderung) übersandt. Ich bezweifle, ob der 3 Jahre alte Bericht, der für einen völlig anderen Zweck (Kostenübernahme für eine Heimunterbringung) gefertigt wurde, geeignet war, die aktuelle Arbeitsfähigkeit des Hilfeempfängers zu beurteilen. Ungeachtet dessen hätten die Unterlagen mit den sensiblen medizinischen Daten unmittelbar dem begutachtenden Gesundheitsamt – ohne den Umweg über die Kreisverwaltung – zugeleitet werden müssen. Zudem wurde gegen die Vorschrift des § 76 SGB X verstoßen, die bei einer Übermittlung besonders schutzwürdiger Sozialdaten zusätzlich zu beachten ist. So hätte der Betroffene auf sein Widerspruchsrecht hingewiesen werden müssen.

- Der oben genannte, bereits an mehrere Stellen verteilte Sozialmedizinische Bericht wurde auch dem Hauptamt der Gemeinde überlassen, das ihn für eine Stellungnahme an die Kommunalaufsichtsbehörde verwendete. Der Betroffene hatte beim Innenministerium eine Beschwerde eingelegt, die nicht in unmittelbarem Zusammenhang mit der Sozialhilfegewährung stand. Auch diese Datenübermittlung war unzulässig.

- Der Hilfeempfänger hatte beim Sozialamt schriftlich um Auskunft über die zu seiner Person gespeicherten Daten gebeten. Außerdem wollte er wissen, an welche Stellen Daten übermittelt wurden und welcher Herkunft die gespeicherten Daten sind. Die Gemeinde hat ihm daraufhin zwar einen Computerausdruck zugeleitet, die übrigen Fragen allerdings nicht beantwortet, obwohl er nach § 83 SGB X auch diese Informationen beanspruchen kann.

Die Gemeinde hat in ihrer Stellungnahme die Verstöße gegen datenschutzrechtliche Vorschriften eingeräumt und zugesichert, künftig die Bestimmungen des SGB X zu beachten.

10.6 Berechtigung zum Lesen der Versicherungskonten bei der Landesversicherungsanstalt für das Saarland

Durch einen Hinweis wurde ich darauf aufmerksam, dass im Büro der Selbstverwaltung der LVA für das Saarland zwei Bedienstete die Berechtigung zum lesenden Zugriff auf die Versicherungskonten aller Rentenversicherten hatten.

Dazu muss man wissen, dass die Aufgabe dieses Büros der Selbstverwaltung im Wesentlichen darin besteht, die Selbstverwaltungsorgane – die Vertreterversammlung und den Vorstand – in ihrer ehrenamtlichen Tätigkeit zu unterstützen. In dem Versicherungskonto werden alle Daten gespeichert, die für die Durchführung der Rentenversicherung sowie die Feststellung und Erbringung von Leistungen erforderlich sind, wie z.B. Art und Dauer von Beschäftigungsverhältnissen, Höhe des Verdienstes, Art und Dauer von Erkrankungen. Es stellte sich für mich konkret die Frage, inwiefern es die Aufgabenbestellung der Bediensteten des Büros der Selbstverwaltung rechtfertigt, auf einen solchen sensiblen Datenbestand Zugriff – wenn auch nur mit der Berechtigung zum Lesen – zu nehmen.

Die LVA hat mir als Begründung genannt, dass es auch zu den Aufgaben der Bediensteten des Büros der Selbstverwaltung gehöre, die Versichertenältesten bei ihrer Tätigkeit zu unterstützen. Deren Beratungstätigkeit, wie z.B. Hilfestellung bei Leistungsanträgen oder beim Beschaffen erforderlicher Unterlagen, mache es im Einzelfall erforderlich, die gespeicherten Sozialdaten aus dem Versicherungskonto zu nutzen. Dieser erforderliche Zugriff werde den Versichertenältesten durch die Bediensteten des Selbstverwaltungsbüros verschafft.

Diese Begründung der LVA für das Saarland hat mich allerdings nicht überzeugt. Ich habe die Auffassung vertreten, dass sich der Versichertenälteste, soweit es für die Beratung eines Versicherten tatsächlich einmal erforderlich sein sollte, an den zuständigen Sachbearbeiter wenden könne, der für die Bearbeitung des Falles zuständig ist und somit ohnehin Zugriff auf das jeweilige Versicherungskonto hat. Ich habe hingewiesen auf § 35 Abs. 1 Satz 2 SGB I, wonach die Wahrung des Sozialgeheimnisses die Verpflichtung umfasst, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind und nur an diese weitergegeben werden. Befugt im Sinne dieser Vorschrift sind nur diejenigen Mitarbeiter, die nach der internen Organisation für die Bearbeitung des einzelnen Falles zuständig sind und die die Daten benötigen, um die ihnen übertragenen Aufgaben ordnungsgemäß wahrnehmen zu können. Einschlägig ist in diesem Zusammenhang auch der am 23.5.2001 neu in das Sozialgesetzbuch X aufgenommene § 78 b, wonach sich die Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten hat, keine oder so wenig Sozialdaten wie möglich zu nutzen. Bestätigt in meiner Auffassung, wonach die Zugriffsmöglichkeit für Mitarbeiter des Büros der Selbstverwaltung nicht erforderlich ist, wurde ich durch Informationen, nach denen solche Zugriffe in der Vergangenheit nur sehr selten erfolgt sind.

Auf meine Intervention hin wurden die Zugriffsrechte für die Mitarbeiter des Büros der Selbstverwaltung entzogen. Die Unterstützung der Versichertenältesten wurde in datenschutzgerechter Art und Weise geregelt.

10.7 Datenpool in der gesetzlichen Krankenversicherung

Die gesetzlichen Krankenkassen erhalten – im Wesentlichen für Zwecke der Abrechnung – unter anderem Arbeitsunfähigkeitsbescheinigungen mit Diagnosen, Krankenhausabrechnungen mit Diagnosen, Arzneimittelabrechnungsdaten, Abrechnungen über Heil- und Hilfsmittel mit Diagnosen.

Es besteht seit langem die Forderung der gesetzlichen Krankenkassen, der Forschung, der Gesundheitsberichterstattung sowie der Politik auf Bundes- und Landesebene, diese Daten kassenarten- und sektorübergreifend für eine effektive Aufgabenwahrnehmung zu nutzen.

Für die Steuerung des Gesundheitswesens im Vertragsbereich, für die Qualitätssicherung, die Stärkung der Wirtschaftlichkeit der Versorgung und damit die Optimierung der Behandlung der Versicherten werden diese Daten benötigt.

Es soll deshalb ein Datenpool geschaffen werden – entsprechende Entwürfe für ein so genanntes „Transparenzgesetz“ wurden bereits vorgelegt –, der den verschiedenen Beteiligten als Informationsbasis zur Verfügung stehen soll.

Auch die Datenschutzbeauftragten bestreiten nicht die Sinnhaftigkeit eines solchen Datenpools, sind aber der Auffassung, dass personenbezogene Daten in diesem Zusammenhang nicht erforderlich sind, sondern dass stattdessen die Vorhaltung pseudonymisierter Daten ausreichend sei. Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Neben der grundsätzlichen Forderung, dass die Versichertendaten in dem Datenpool nur in pseudonymisierter Form gespeichert werden dürfen, halten die Datenschutzbeauftragten folgende Punkte für besonders wesentlich:

- Die Zwecke der Datenaufbereitung sind im Gesetz abschließend festzulegen.
- Strikte räumliche, organisatorische und personelle Trennung der Vertrauensstellen – das sind die Stellen, die die Versichertendaten pseudonymisieren – und der Datenaufbereitungsstellen – des eigentlichen Datenpools – von den Krankenkassen und deren Verbänden, den kassenärztlichen Vereinigungen und sonstigen abrufberechtigten Stellen.
- Es muss ein sicheres Pseudonymisierungsverfahren eingesetzt werden und der Umfang der Datenübermittlung so begrenzt werden, dass ein Reidentifizierungsrisiko minimiert ist.
- Festlegung der bei den Datenaufbereitungsstellen gespeicherten Daten durch Rechtsverordnung
- Regelung, dass nur aggregierte Auswertungen zulässig sind; Ausschluss des Zugriffs auf einzelne Datensätze und von Auswertungen, die Rückschlüsse auf einzelne Personen zulassen.
- Sowohl für die Vertrauensstelle als auch die Datenaufbereitungsstelle ist die öffentliche Rechtsform vorzusehen; Klarstellung, dass Vertrauensstelle und Datenaufbereitungsstelle Stellen im Sinne des § 35 SGB I sind.

10.8 Medikamenten-Chipkarte

Im Zusammenhang mit der Lipobay-Affäre sind Pläne des Bundesgesundheitsministeriums zur Einführung einer Medikamenten-Chipkarte bekannt geworden.

Auf der Karte sollten alle ärztlichen Verordnungen gespeichert werden. Ärzte und Apotheker, denen die Karte vorgelegt wird, sollten so einen vollständigen Überblick über Medikamente erhalten, die ein Patient einnimmt. Es sollten damit vor allen Dingen unerwünschte Wechselwirkungen verschiedener Medikamente vermieden werden. Im Verlauf der Diskussion wurden Überlegungen in die Öffentlichkeit getragen, weitere Gesundheits- und Behandlungsdaten auf der Karte zu speichern.

Aus datenschutzrechtlicher Sicht besteht die Problematik solcher Karten allerdings darin, dass sich aus ihr eine umfassende Information über den Gesundheitszustand einer Person ergibt – aus der Art eines Medikamentes lassen sich Rückschlüsse auf die zugrunde liegende Krankheit ziehen. Bei jeder Vorlage der Karte ist man damit faktisch gezwungen, seine gesamten Krankheiten zu offenbaren.

Eine zentrale Forderung der Datenschutzbeauftragten des Bundes und der Länder lautet deshalb, dass es der freien Entscheidung jedes Einzelnen überlassen bleiben muss, ob er die Karte verwenden will. Dazu gehört auch, dass die Betroffenen entscheiden können,

- ob ihre Daten auf einer Chipkarte gespeichert werden,
- welche ihrer Gesundheitsdaten auf die Karte aufgenommen werden,
- welche ihrer Daten auf der Karte wieder gelöscht werden,
- ob sie die Karte bei einem Arzt oder Apothekenbesuch vorlegen und
- welche ihrer Daten sie im Einzelfall zugänglich machen (die Technik muss eine partielle Freigabe ermöglichen).

Diese und andere Gesichtspunkte, die im Zusammenhang mit Überlegungen zur Einführung einer solchen Karte zu beachten sind, haben die Datenschutzbeauftragten des Bundes und der Länder auf ihrer Konferenz vom 24. bis 26. Oktober 2001 in einer Entschließung zusammengefasst (siehe Anlage 11).

10.9 Disease-Management-Programme der Krankenkassen

Seit die Versicherten ihre Krankenkasse frei wählen können, hat ein Wettbewerb unter den Krankenkassen eingesetzt, der dazu geführt hat, dass die Krankenkassen ihr Augenmerk auf die „guten Risiken“ (junge, gut verdienende Beitragszahler) gelegt haben. Um dieser Entwicklung gegenzusteuern, kam der Gesetzgeber auf die Idee, so genannte Disease-Management-Programme (DMP) für chronisch Kranke einzuführen. Ein Disease-Management-Programm ist die abgestimmte Behandlung und Betreuung der Patienten nach Kriterien, die auf den Leitlinien der medizinischen Fachgesellschaften beruhen. Dadurch, dass die Kassen für jeden in einem DMP eingeschriebenen Patienten dessen durchschnittliche Kosten aus dem Risikostrukturausgleich ersetzt bekommen, rechnen sie mit Einsparungseffekten.

Die Datenschutzbeauftragten des Bundes und der Länder haben frühzeitig die Gefahr gesehen, dass im Zusammenhang mit der Durchführung dieser Programme für einen Teil der Versicherten, nämlich die chronisch Kranken, der „gläserne Versicherte“ entstehen könnte. Denn da die einzelnen Krankenkassen zu Lasten anderer Krankenkassen aus der Teilnahme ihrer Versicherten an DMPen erhebliche Ansprüche im Risikostrukturausgleich geltend machen können, ist eine Mitverantwortung der Krankenkassen für die ordnungsgemäße Durchführung der DMPe und damit verbunden in gewissem Umfang auch durch Verarbeitung personenbezogener Daten die Behandlung überprüfen zu können, nicht von der Hand zu weisen.

Im Rahmen des Gesetzgebungsverfahrens konnte erreicht werden, dass die Teilnahme von Versicherten an diesen strukturierten Behandlungsprogrammen freiwillig ist und die zu deren Durchführung erforderlichen Daten von den Krankenkassen vor allem nur dann erhoben, verarbeitet und genutzt werden dürfen, wenn der Versicherte auf der Grundlage einer umfassenden Information durch die Krankenkasse hierin eingewilligt hat. Erreicht werden konnte auch, dass Art und Umfang der betroffenen Daten in einer Verordnung zu regeln sind. Die vierte Verordnung zur Änderung der Risikostruktur-Ausgleichsverordnung ist mittlerweile am 1. Juli 2002 in Kraft getreten. Diese regelt nunmehr detailliert, wie die Versichertendaten im Rahmen der Disease-Management-Programme zu verarbeiten sind. Aufgabe der Datenschutzbeauftragten wird es sein, die Handhabung der Befugnisse der Krankenkassen im Zusammenhang mit den DMPen zu kontrollieren.

10.10 Auskunfts-/Akteneinsichtsrechte

Immer wieder beschweren sich Petenten bei meiner Dienststelle darüber, dass ihnen von Behörden eine Einsicht in die über ihre Person geführte Akte oder die Auskunft über gespeicherte Daten verweigert wird. Die betreffenden Behörden rechtfertigen ihre Ablehnung mit den unterschiedlichsten Gründen: Es verstoße gegen den Datenschutz, wenn die gewünschte Auskunft erteilt werde. Bei der Vielzahl der geführten Akten bedeute es einen unzumutbaren Aufwand, wenn jedem Bürger Auskunft erteilt werden müsse. Häufig zu hören ist auch das Argument, die Informationen seien auch bei anderen Stellen gespeichert; der Betroffene möge sein Auskunftsbegehren dort geltend machen.

Ich muss zugeben, dass es mich schon erstaunt, wie ablehnend sich viele Behörden gegenüber Anträgen auf Akteneinsicht oder Auskünften über gespeicherte Daten verhalten. Denn das Auskunftsrecht des Bürgers über die zu seiner Person gespeicherten Daten ist sowohl im Landesdatenschutzgesetz (§ 20 SDSG) als auch in einer Vielzahl bereichsspezifischer Vorschriften (z.B. § 83 SGB X für den Sozialleistungsbereich, § 22 Saarländisches Gesundheitsdienstgesetz, § 29 Krankenhausgesetz) ausdrücklich normiert. So heißt es etwa in § 20 SDSG: „Dem Betroffenen ist von der verantwortlichen Stelle auf Antrag unentgeltlich Auskunft zu erteilen über die zu seiner Person gespeicherten Daten, den Zweck und die Rechtsgrundlage der Verarbeitung sowie die Herkunft der Daten und die Empfänger von Übermittlungen, soweit dies gespeichert ist.“

Es gibt zwar auch Ausnahmen von dieser grundsätzlichen Pflicht zur Auskunftserteilung; es ist nur so, dass bisher keiner dieser Ausnahmetatbestände in den an mich herangetragenen Fällen vorgelegen hat. Ich habe vielmehr den Eindruck, dass man sich in vielen Behörden der grundsätzlich bestehenden Auskunftsrechte nicht bewusst ist.

Folgende Beispielsfälle aus meiner Datenschutzpraxis möchte ich im Folgenden schildern:

Ein Petent hatte beim Landesamt für Verbraucher-, Gesundheits- und Arbeitsschutz Einsicht in die über ihn im Rahmen eines Berufskrankheitenverfahrens geführte Akte beantragt (das Landesamt für Verbraucher-, Gesundheits- und Arbeitsschutz wird im Rahmen des Berufskrankheitenverfahrens als Gutachterstelle für die Berufsgenossenschaften tätig). Die zuständige Abteilung des betreffenden Amtes steht auf dem Standpunkt, die Akteneinsicht sei für die Geltendmachung rechtlicher Interessen des Antragstellers nicht erforderlich, weil Herr des Verfahrens der Unfallversicherungsträger sei, die Gutachten isoliert nicht anfechtbar seien. Dem Antragssteller fehle mithin für einen Akteneinsichts- bzw. Auskunftsanspruch das Rechtsschutzbedürfnis.

Ich habe demgegenüber die Auffassung vertreten, dass der Antragsteller seinen Auskunftsanspruch auf § 83 SGB X stützen könne. Denn diese Vorschrift ist Ausfluss des Rechtes auf informationelle Selbstbestimmung, nach dem eine „Gesellschaftsordnung und eine dies ermöglichende Rechtsordnung gegen die Rechte aus Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 Grundgesetz verstoßen würde, wenn der Bürger nicht mehr erfahren kann, wer, was, wann und bei welcher Gelegenheit über ihn weiß“ (BVerfGE 65, 1, 42 f.). Es kommt also gerade nicht darauf an, ob der Betroffene die Akteneinsicht zur Geltendmachung seiner rechtlichen Interessen benötigt.

Das Landesamt für Verbraucher-, Gesundheits- und Arbeitsschutz hat in dem konkreten Einzelfall die gewünschte Akteneinsicht erteilt. Ob man dort bereit ist, generell von der Rechtsansicht abzurücken, im Berufskrankheitenverfahren bestehe ein Auskunftsanspruch lediglich gegenüber dem Unfallversicherungsträger, war bei Redaktionsschluss noch nicht bekannt.

In einem anderen Fall ging es darum, dass ein Antragssteller von der Kassenärztlichen Vereinigung wissen wollte, welche Daten dort im Einzelnen über seine Person gespeichert sind. Im Rahmen der Abrechnung ärztlicher Leistungen verfügt die Kassenärztliche Vereinigung über die Information, welche Leistungen aufgrund welcher Diagnose ein Arzt bei dem einzelnen Patienten erbracht hat.

Die Kassenärztliche Vereinigung hatte den Antrag zunächst abschlägig beschieden mit der Begründung, der Antragsteller solle sich an seine Krankenkasse wenden und dort seinen Auskunftsanspruch gemäß § 305 Abs. 1 SGB V geltend machen. Nach dieser Vorschrift unterrichten die Krankenkassen die Versicherten auf deren Antrag über die im jeweils letzten Geschäftsjahr in Anspruch genommenen Leistungen und deren Kosten. Die Kassenärztlichen Vereinigungen übermitteln den Krankenkassen zu diesem Zweck die Angaben über die von dem Versicherten in Anspruch genommenen ärztlichen Leistungen.

Ich habe die Auffassung vertreten, dass der Auskunftsanspruch gemäß § 305 SGB V – gegenüber der Krankenkasse – und der Anspruch gemäß § 83 SGB X – gegenüber der Kassenärztlichen Vereinigung – nebeneinander bestehen. Denn der Gesetzgeber verfolgt mit der Einräumung der Auskunftsrechte unterschiedliche Zwecke. Während es bei § 83 SGB X darum geht, den Anspruch des Betroffenen auf Verwirklichung seines Rechts auf informationelle Selbstbestimmung zu verwirklichen, verfolgt § 305 Abs. 1 SGB V demgegenüber den gesundheitspolitischen Zweck der Transparenz über das Leistungsgeschehen gegenüber den Versicherten.

Aufgrund meiner Intervention hat die Kassenärztliche Vereinigung die gewünschten Auskünfte zwischenzeitlich erteilt.

11 Gesundheit

11.1 Unterbringungsdatei psychisch Kranker beim Ordnungsamt

Das Ordnungsamt einer Stadt führt eine automatisierte Datei aller Personen, für die es nach dem saarländischen Unterbringungsgesetz einen richterlichen Beschluss zur zwangsweisen Unterbringung in einem psychiatrischen Krankenhaus beantragt hat. Gespeichert war neben den Personalien u. a. auch eine Kurzfassung des ärztlichen Gutachtens. Eine Löschung der Daten war erst nach dem Tod des Betroffenen vorgesehen. Mit der Datei soll die Erstellung der Anträge bei Verlängerung oder erneuter Unterbringung sowie die Auskunftserteilung, z.B. an die Polizei in einer Gefahrensituation, erleichtert werden.

Ich halte es für problematisch, wenn solch sensible Daten – neben der weiterhin vorhandenen Akte - zeitlebens automatisiert gespeichert werden. Es stellt sich die Frage, ob eine solche Verfahrensweise mit dem Gebot in § 3 Unterbringungsgesetz, die Persönlichkeitsrechte der betroffenen Personen zu wahren, vereinbar ist. Ich hätte es vorgezogen, wenn in der Datei nur Hinweise auf die Akten gespeichert würden.

Die Stadt hat sich schließlich bereit erklärt, die medizinischen Daten ein Jahr nach Erlass des Unterbringungsbeschlusses, die übrigen Daten 10 Jahre nach dem Abschluss des Falles zu löschen.

11.2 Vorlage des kompletten Unterbringungsbeschlusses für die Kostenübernahme

Ein Krankenhausarzt hatte mich darauf hingewiesen, dass der Sozialhilfeträger im Kostenübernahmeantrag für die stationäre Behandlung eines zwangsweise Untergebrachten verlangt, stets den gerichtlichen Unterbringungsbeschluss beizufügen. Nach seiner Auffassung sollte genügen, für die Aufnahme im Krankenhaus eine medizinische Indikation nachzuweisen. Meine Feststellungen haben ergeben, dass nach einer Regelung im saarländischen Ausführungsgesetz zum Bundessozialhilfegesetz der überörtliche Träger der Sozialhilfe (das ist das Landesamt für Jugend, Soziales und Versorgung) für die Kostenübernahme eines zwangsweise untergebrachten psychisch Kranken zuständig ist. Dieses Amt benötigt zur Prüfung, ob diese Voraussetzung gegeben ist, den Gerichtsbeschluss. Die Sozialbehörden dürfen allerdings nur die Daten erheben, deren Kenntnis zur Aufgabenerfüllung erforderlich, d.h. unerlässlich ist. Die Kenntnis des gesamten Beschlusses, in dem häufig die medizinischen, familiären und sozialen Verhältnisse des Betroffenen detailliert dargestellt sind, wird regelmäßig für die Kostenentscheidung nicht benötigt. Ich habe vorgeschlagen, dem Kostenübernahmeantrag nur die erste Seite des Gerichtsbeschlusses beizufügen. Das Landesamt hat dieser Lösung zugestimmt, wenn sichergestellt ist, dass aus der ersten Seite die Personalien des Betroffenen, die Dauer der Unterbringung sowie der Name der Einrichtung zu entnehmen sind.

11.3 Impfkontrolle beim Gesundheitsamt

Ob Eltern ihre Kinder impfen lassen, ist deren freiwillige Entscheidung; es besteht keine Impfpflicht. Eltern sind demzufolge rechtlich auch nicht verpflichtet, Daten über den Impfschutz ihrer Kinder dem Gesundheitsamt bekannt zu geben oder das Impfbuch vorzulegen. Ebenso dürfen Impfdaten beim Gesundheitsamt nur auf freiwilliger Grundlage gespeichert werden.

Eltern haben mir das Schreiben eines Gesundheitsamtes mit dem Angebot eines Impftermins in der Schule vorgelegt. Die Eltern werden darin gebeten, sich vom Kinderarzt oder Hausarzt in einem Vordruck die durchgeführten und geplanten Impfungen bescheinigen zu lassen und die "Impfrückmeldung" dem Gesundheitsamt zuzusenden.

Das Ministerium für Frauen, Arbeit, Gesundheit und Soziales ging als Fachaufsichtsbehörde zunächst davon aus, dass die Freiwilligkeit bereits ausreichend darin zum Ausdruck kommt, dass die Datenerhebung des Gesundheitsamtes als "Bitte" formuliert ist. Diese Auffassung kann ich nicht teilen. Datenanforderungen öffentlicher Stellen werden heute regelmäßig – auch wenn eine gesetzliche Auskunftspflicht statuiert ist – mit dem Verb "bitten" versehen. Dies gebietet der höfliche Umgang der Behörde mit dem Bürger. Wenn der Bürger rechtlich nicht verpflichtet ist, Daten anzugeben, sollte die Datenerhebung ausdrücklich als "freiwillig" bezeichnet werden. Mit dem Ministerium wurde Einvernehmen erzielt, dass das Anforderungsschreiben entsprechend geändert wird.

11.4 Einsichtsbefugnis der Krankenhausverwaltung (Medizin-Controller) in Krankenakten

Der Datenschutzbeauftragte eines Krankenhauses wollte meine Auffassung zu der Frage wissen, ob und in welchem Umfang Mitarbeiter der Krankenhausverwaltung Einsicht in Patientenunterlagen nehmen dürfen. Konkret hatte man in dem betreffenden Krankenhaus überlegt, einem so genannten „Medizin-Controller“ u.a. die Aufgabe zu übertragen, durch Einsichtnahme in Krankenakten zu überprüfen, ob die ärztlichen und pflegerischen Leistungen ordnungsgemäß dokumentiert werden.

Ich habe darauf hingewiesen, dass Ausgangspunkt aller Überlegungen in diesem Zusammenhang die Wertung des Gesetzgebers sein muss, dass ein Krankenhaus keine rechtliche Einheit ist, innerhalb deren personenbezogene Patientendaten beliebig offenbart werden dürfen. Dieser Gedanke findet seinen Niederschlag konkret in der Vorschrift des § 29 Saarländisches Krankenhausgesetz über den Patientendatenschutz, wenn es dort heißt:

- Die Weitergabe von Patientendaten an andere Fachabteilungen innerhalb des Krankenhauses oder an den Sozialdienst im Krankenhaus ist nur zulässig, soweit sie für die Behandlung oder soziale Betreuung des Patienten erforderlich ist (§ 29 Abs. 3 Satz 1 SKHG).

- Die im Krankenhaus Beschäftigten dürfen Patientendaten für den zur jeweiligen Aufgabenerfüllung gehörenden Behandlungszweck einsehen oder sonst nutzen (§ 29 Abs. 3 Satz 3 SKHG).

- Die Nutzung der Patientendaten durch die Krankenhausverwaltung darf nur in dem Maße erfolgen, wie dies für die Abwicklung des Behandlungsfalles erforderlich ist (§ 29 Abs. 3 Satz 4 SKHG)

Der Krankenhausverwaltung dürfen deshalb nur Patientendaten für die Abwicklung des Behandlungsfalles, womit insbesondere die Abrechnung mit den Kostenträgern gemeint ist, zur Verfügung gestellt werden. Ich habe im Übrigen auf § 34 des Saarländischen Krankenhausgesetzes hingewiesen, nach dessen Absatz 2 Nr. 4 die Sicherstellung der ärztlichen Aufzeichnung und Dokumentation eine Aufgabe des ärztlichen Direktors ist.

11.5 Verwaltungsvorschriften im Maßregelvollzug

Das Ministerium für Frauen, Arbeit, Gesundheit und Soziales hat verständlicherweise die Bedingungen verschärft, unter denen Patienten im Maßregelvollzug, die schwere Straftaten begangen hatten, erstmals Ausgang, Freigang oder andere Lockerungen des Vollzugs gewährt wird. Durch Verwaltungsvorschrift wurde angeordnet, dass in bestimmten Fällen ein Gutachter hinzuzuziehen ist, der außerhalb der Einrichtung arbeitet, vom Träger unabhängig ist und über die für eine Begutachtung erforderliche forensisch-psychiatrische Berufserfahrung verfügt. Die Beauftragung eines externen Gutachters macht es notwendig, dass detaillierte Patientendaten an einen Außenstehenden übermittelt werden.

Ich habe das Ministerium darauf hingewiesen, dass im Maßregelvollzugsgesetz spezielle Regelungen über den Patientendatenschutz getroffen wurden und dass die Datenübermittlung an einen externen Gutachter darin keine gesetzliche Grundlage hat. Deshalb habe ich vorgeschlagen, in der Verwaltungsvorschrift einen Hinweis aufzunehmen, dass der Patient seine Einwilligung zu erteilen hat. Die Hausspitze des Ministeriums hat mir lediglich lapidar mitgeteilt, meine Beanstandung sei unbegründet und es werde kein weiterer Handlungsbedarf gesehen. Nach nochmaliger Intervention wurde mir mit gleichem Wortlaut geantwortet.

Unabhängig davon, wie man zu der Angelegenheit steht, kann der Landesbeauftragte für Datenschutz erwarten, dass das Ministerium sich sachlich mit den vorgetragenen Argumenten auseinandersetzt und - falls es diese nicht teilt - zumindest die Gründe für eine andere Auffassung bekannt gibt. Alles andere ist schon deshalb nicht hinnehmbar, weil der Landesbeauftragte für Datenschutz letztlich einen Teil der parlamentarischen Kontrollfunktion des saarländischen Landtages als Vertreter der Bürgerinnen und Bürger dieses Landes wahrnimmt. Eine solche Verhaltensweise ist mir zudem von den anderen obersten Landesbehörden, von anderen öffentlichen Stellen und auch von der Arbeitsebene des betroffenen Ministeriums bisher gänzlich unbekannt.

Erstaunlich erscheint auch, dass das Ministerium eine Änderung des Maßregelvollzugsgesetzes in anderem Zusammenhang nicht zum Anlass genommen hat, die strittige Datenverarbeitung auf eine gesicherte Rechtsgrundlage zu stellen.

11.6 Medizinnetze

Eine Arbeitsgruppe des Arbeitskreises „Technik“ und des Arbeitskreises „Gesundheit und Soziales“ der Konferenz der Datenschutzbeauftragten hat ein Papier „Datenschutz und Telemedizin – Anforderungen an Medizinnetze“ erarbeitet.

Die Ausarbeitung setzt sich mit den allgemeinen datenschutzrechtlichen Anforderungen bei Medizinnetzen auseinander, insbesondere den Rechtsgrundlagen, der Dokumentationspflicht, der Befugnis zur Übermittlung bzw. Weitergabe von Patientendaten, den Informationsrechten des Patienten, der Datenverarbeitung im Auftrag durch externe Dritte und dem Abruf von Patientendaten über ein Datennetz. Weiter sind in dem Papier Ausführungen zu den grundlegenden Sicherheitsanforderungen enthalten, wie der Vertraulichkeit, der Authentizität, der Integrität, der Verfügbarkeit, der Revisionsfähigkeit, der Validität, der Rechtssicherheit, der Nichtabstreitbarkeit von Datenübermittlungen und der Nutzungsfestlegung. Zu diesen Punkten finden sich auch Erläuterungen hinsichtlich der speziellen Datensicherheitsmaßnahmen in technischer Hinsicht. Verschiedene Modelle dieser neuen Verfahren werden in diesem Papier dargestellt und datenschutzrechtlich bewertet.

Ich habe das Papier unter meiner Internet-Adresse www.lfd.saarland.de veröffentlicht.

11.7 Saarländisches Bestattungsgesetz

Im Berichtszeitraum wurde mir vom saarländischen Ministerium für Frauen, Arbeit, Gesundheit und Soziales der Entwurf eines Gesetzes über das Friedhofs-, Bestattungs- und Leichenwesen zur Stellungnahme aus datenschutzrechtlicher Sicht vorgelegt.

Man mag sich fragen, was ein Gesetz, das sich unter anderem mit der Anlegung und Unterhaltung von Friedhöfen, den Anforderungen an Bestattungseinrichtungen oder der Leichenbeförderung befasst, mit dem Datenschutz zu tun hat. Die Antwort liegt darin, dass Gegenstand des Bestattungsgesetzes auch die Durchführung der Leichenschau und damit verbunden die Ausstellung des Leichenschauscheines ist. Neben der Feststellung des Todes sowie des Todeszeitpunktes ist Inhalt des Leichenschauscheines auch die Todesart und die Todesursache. Es wird beispielsweise eingetragen, welche Krankheit den Tod herbeigeführt hat, welche anderen Krankheiten zur Zeit des Todes bestanden, ob Ursache des Todes eine Selbsttötung war oder ob eine Verstorbene schwanger war. Unter den Gesichtspunkten der ärztlichen Schweigepflicht, der Achtung der Menschenwürde und auch des Schutzes der Angehörigen der Verstorbenen sind Regelungen über den Umgang mit den Leichenschauscheinen erforderlich. Für regelungsbedürftig halte ich die Festlegung der Zwecke des Leichenschauscheins, die Voraussetzungen, unter denen Auskünfte aus dem Leichenschauschein erteilt werden dürfen sowie die Dauer der Aufbewahrung.

So wurde ich in meiner datenschutzrechtlichen Praxis immer wieder mit der Frage befasst, ob und unter welchen Voraussetzungen der Leichenschauschein zu Forschungszwecken genutzt werden darf. Auch habe ich des Öfteren Anfragen von Angehörigen Verstorbener erhalten, die zu unterschiedlichen Zwecken, etwa zur Klärung von Versicherungsleistungen oder auch nur um Gewissheit über die Todesursache ihres Angehörigen zu haben, Einsicht in die Leichenschauscheine nehmen wollten.

Ich hätte eigentlich erwartet, dass die angesprochenen Punkte Gegenstand des vorliegenden Gesetzentwurfes sind. Denn wegen der Schwere des Eingriffs durch Informationsweitergabe und unter dem Gesichtspunkt, dass hier durchaus strittige Fragen zur Diskussion stehen, halte ich eine Entscheidung durch den Gesetzgeber erforderlich; die vom Gesetz vorgesehene Regelung durch Rechtsverordnung ist nicht ausreichend. In einer Rechtsverordnung könnten allenfalls die Details geregelt werden, wie etwa Inhalt des Leichenschauscheines oder Aufzählung der Behörden, die den Leichenschauschein regelmäßig zu ihrer Aufgabenerfüllung erhalten.

Eine Umfrage bei den Datenschutzbeauftragten der anderen Bundesländer hat ergeben, dass in den meisten Bundesländern die angesprochenen Fragen gesetzlich geregelt sind.

In meiner Stellungnahme habe ich konkrete Formulierungsvorschläge gemacht. Bei der Frage etwa, welchen Personen und Stellen Auskunft aus den Leichenschauscheinen gegeben werden darf, habe ich vorgeschlagen zwischen Angehörigen, sonstigen Antragsstellern und Forschern zu differenzieren. So sollten Angehörige die Auskunft bei Vorliegen eines berechtigten Interesses erhalten, während ich bei sonstigen Antragstellern ein rechtliches Interesse an der Kenntnis von Daten aus dem Leichenschauschein für angemessen halte. Forscher sollten Zugang zu den Daten erhalten, wenn das für das Gesundheitswesen zuständige Ministerium feststellt, dass das öffentliche Interesse an dem Forschungsvorhaben das Geheimhaltungsinteresse des Verstorbenen und seiner Angehörigen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Ich hoffe, dass meinen Forderungen im Laufe des Gesetzgebungsverfahrens noch Rechnung getragen wird.

12 Forschung

12.1 Saarländisches Krebsregistergesetz

Im Berichtszeitraum war es endlich soweit: Das Saarländische Krebsregistergesetz aus dem Jahre 1979 wurde aufgehoben und durch ein neues Krebsregistergesetz ersetzt. Meine Kritik gegen das ursprüngliche Gesetz hatte sich vor allem dagegen gerichtet, dass die Meldungen der Ärzte über eine Krebserkrankung an das Krebsregister ohne jegliche Beteiligung der Patienten – die Patienten wussten nicht einmal etwas von einer solchen Meldung – erfolgte. Für unbefriedigend hatte ich auch die verfahrensrechtlichen Vorkehrungen gehalten, die verhindern sollten, dass die grundsätzlich getrennt gespeicherten Identitätsdaten und Krankheitsdaten wieder personenbezogen zusammengeführt werden konnten. Auch der Umstand, dass eine Nutzung der Daten zu Forschungszwecken äußerst restriktiv geregelt war, hat mich in der Vergangenheit immer wieder veranlasst, eine Novellierung anzumahnen. Denn immer wieder wurde dem „Datenschutz“ der Vorwurf der Forschungsfeindlichkeit gemacht, obwohl hier eindeutige Versäumnisse des Gesetzgebers vorlagen.

Mit dem im April 2002 in Kraft getretenen neuen Krebsregistergesetz ist es meiner Auffassung nach im Wesentlichen gelungen – auf Kritikpunkte werde ich im Folgenden noch eingehen – eine effektive und zugleich datenschutzgerechte Gestaltung des Krebsregisters zu verwirklichen.

So sind nunmehr die meldenden Ärzte verpflichtet, die Patientin oder den Patienten vor einer beabsichtigten Meldung an das Krebsregister zu unterrichten. Die Patientin bzw. der Patient ist gleichzeitig darüber zu informieren, dass sie bzw. er das Recht hat, der Meldung zu widersprechen. Unterrichtung und Information dürfen nur unterbleiben, solange der begründete Verdacht besteht, dass der Patientin oder dem Patienten bei vorheriger Unterrichtung weitere schwerwiegende gesundheitliche Nachteile entstehen. Von dem Grundsatz, dass die Patientin bzw. der Patient vor der Meldung an das Krebsregister unterrichtet wird, macht das Gesetz für Pathologinnen und Pathologen eine Ausnahme. Diese sind auch ohne vorherige Unterrichtung der Patientin oder des Patienten zur Meldung berechtigt. Da nach den bisherigen Erfahrungen des Saarländischen Krebsregisters der überwiegende Teil der Meldungen von diesem Personenkreis stammt, habe ich gegen diese Regelung keine durchgreifenden Bedenken erhoben, obwohl ich mir bewusst bin, dass dadurch der Grundsatz der vorherigen Unterrichtung der Patienten stark relativiert wird. Meine Bedenken habe ich auch unter dem Gesichtspunkt zurückgestellt, dass die Patientin bzw. der Patient auf jeden Fall vom behandelnden Arzt nachträglich zu unterrichten ist und die Patientin oder der Patient das Recht hat, bereits gemeldete Daten wieder löschen zu lassen.

Was die Speicherung der Daten im Krebsregister betrifft, liegt dem Krebsregistergesetz die Idee zugrunde, dass die Daten zwar personenbezogen zum Krebsregister gemeldet werden, dort dann aber so verarbeitet werden, dass eine Identifizierung einzelner Personen grundsätzlich nicht möglich ist. Hierzu sieht das Gesetz die Bildung von zwei verschiedenen Organisationseinheiten vor: die Vertrauensstelle und die Registerstelle. In der Vertrauensstelle werden die verschlüsselten Identitätsdaten gespeichert, in der Registerstelle die epidemiologischen Daten, also im wesentlichen Gesundheitsdaten wie Tumordiagnose, Zeitpunkt der Diagnose, frühere Tumorleiden, Stadium der Erkrankung, Art der Therapie usw. Diese Aufteilung der Daten auf zwei verschiedene Stellen soll eine Zusammenführung von Identitätsdaten und Gesundheitsdaten erschweren. Deshalb ist in § 2 Abs. 3 des Krebsregistergesetzes bestimmt, dass die Vertrauensstelle und die Registerstelle räumlich, organisatorisch und personell voneinander getrennt und als selbständige Einheiten geführt werden. Allerdings enthält das Gesetz gleichzeitig die Aussage, dass das Krebsregister im Geschäftsbereich des Ministeriums für Frauen, Arbeit, Gesundheit und Soziales geführt wird. In der Praxis ist es so, dass Vertrauensstelle und Registerstelle als Untergliederungen einer größeren Organisationseinheit unter gemeinsamer Leitung innerhalb dieses Ministeriums eingerichtet worden sind. Diese Gestaltung erscheint mir nicht geeignet, der von Gesetzes wegen geforderten Trennung von Vertrauensstelle einerseits und Registerstelle andererseits zu genügen. Im Gesetzgebungsverfahren habe ich deshalb auf die Situation in anderen Bundesländern hingewiesen, wo die Aufgaben dieser beiden Stellen – schon im Gesetz – ausdrücklich unterschiedlichen Institutionen übertragen worden sind. So ist beispielsweise im bayerischen Gesetz zur Ausführung des Krebsregistergesetzes vom 24.11.1997 festgelegt, dass die Vertrauensstelle bei dem pathologischen Institut des Klinikums der Stadt Nürnberg und die Registerstelle beim Klinikum der Friedrich-Alexander-Universität Erlangen-Nürnberg eingerichtet wird. Hessen hat nach dem Krebsregistergesetz vom 31.10.1998 die Vertrauensstelle bei der Landesärztekammer, die Registerstelle beim Regierungspräsidium Darmstadt eingerichtet. In Rheinland-Pfalz (Landeskrebsregistergesetz vom 22. 12.1999) ist die Aufgabe der Vertrauensstelle dem Tumorzentrum e.V., die der Registerstelle dem Institut für Medizinische Statistik und Dokumentation des Klinikums der Johannes-Gutenberg-Universität übertragen. Nach dem Krebsregistergesetz des Landes Schleswig-Holstein vom 28.10.1999 nimmt die Ärztekammer die Aufgaben der Vertrauensstelle und das Institut für Krebsepidemiologie die Aufgaben der Registerstelle war.

Die Freie Hansestadt Bremen hat aufgrund einer Ermächtigung im Bremischen Krebsregistergesetz vom 18.9.1997 durch Rechtsverordnung festgelegt, dass die Vertrauensstelle bei der Kassenärztlichen Vereinigung und die Registerstelle beim Bremer Institut für Präventionsforschung und Sozialmedizin eingerichtet werden.

Als Fazit bleibt festzuhalten, dass die Änderungen bei den Modalitäten des Meldeverfahrens aus datenschutzrechtlicher Sicht sehr zu begrüßen sind. Andererseits halte ich die unzureichende Abschottung zwischen Vertrauensstelle und Registerstelle für einen schwerwiegenden Mangel des neuen Gesetzes.

12.2 Genomanalyse

Der Umgang mit genetischen Daten wirft eine Fülle datenschutzrechtlicher Fragen auf, wie z.B.: Unter welchen Voraussetzungen sind genetische Untersuchungen zu medizinischen Zwecken zulässig? Wie verhält es sich mit Gentests in Arbeits- oder Versicherungsverhältnissen? In welchem Umfang dürfen zur Klärung von Identität und Abstammung entsprechende Untersuchungen durchgeführt werden? Welche Rahmenbedingungen gelten für die Erhebung, Verarbeitung und Nutzung genetischer Daten im Zusammenhang mit Forschungsvorhaben?

Zwar können Antworten durch entsprechende Interpretation der datenschutzrechtlichen Vorschriften gegeben werden; klare Spezialregelungen wären jedoch wünschenswert.

Eine Bund-Länder-Arbeitsgruppe der Datenschutzbeauftragten hat deshalb einen „Regelungsentwurf zu einem Gesetz zur Sicherung der Selbstbestimmung bei genetischen Untersuchungen“ erarbeitet (veröffentlicht in meinem Internet-Angebot www.lfd.saarland.de), der Anregungen geben soll zu anstehenden Gesetzesinitiativen und zur gesellschaftspolitischen Diskussion.

Die Dringlichkeit zur Schaffung bereichsspezifischer Bestimmungen zu den verschiedenen Zwecken genetischer Untersuchungen haben die Datenschutzbeauftragten von Bund und Ländern in einer gemeinsamen Entschließung auf ihrer Konferenz vom 24. bis 26.10.2001 (siehe Anlage12) unterstrichen.

13 Schulen

13.1 Weitergabe von Gesundheitsdaten bei einem Schulwechsel

Eine Petentin hat sich mit folgendem Sachverhalt an meine Dienststelle gewandt:

Die Petentin hat einen Sohn, der an einer epileptischen Erkrankung litt. Die entsprechenden ärztlichen Befunde und Berichte wurden zu den Schulakten genommen.

In der Folgezeit zog die Petentin mit ihrem Sohn in ein anderes Bundesland um, wo ihr Sohn eine andere Schule besuchte. Nach Angaben der Petentin war die Epilepsie zu diesem Zeitpunkt ausgeheilt. Sie wollten deshalb nicht, dass die neue Schule von der früheren Erkrankung Kenntnis erhielt.

Aufgrund entsprechender Äußerungen von Lehrern hatte ihr Sohn jedoch bald den Eindruck, dass seine Krankengeschichte in der neuen Schule doch bekannt war. Dieser Eindruck bestätigte sich, als die Petentin Einsicht in die Schülerunterlagen nahm. Es fanden sich dort Kopien von Unterlagen über die ausgeheilte Erkrankung.

Als die Petentin sich bei der alten Schule deswegen beschwerte, bekam sie zur Antwort, dass ja nur ein Teil der ärztlichen Unterlagen an die neue Schule übersandt worden sei und dass nach saarländischer Gesetzeslage sogar die komplette Schülerakte hätte weitergeleitet werden müssen.

Dieser Interpretation der schulrechtlichen Datenschutzbestimmungen des betreffenden Schulleiters musste ich entschieden widersprechen. Die Rechtslage bei der Weitergabe von Schülerdaten von der bisher besuchten Schule an eine Folgeschule stellt sich vielmehr wie folgt dar: Im Saarland gibt es eine Verordnung über die Erhebung, Verarbeitung und sonstige Nutzung personenbezogener Daten in den Schulen vom 3. November 1986 (Amtsblatt des Saarlandes vom 21. November 1986, Seite 990). In § 7 Abs. 2 Nr. 1 dieser Verordnung ist ausdrücklich festgelegt, dass bei einem Schulwechsel der Schülerbogen, die Schülerakte und die sonstigen schriftlichen Nachweise nicht weitergereicht werden dürfen. Die abgebende Schule übermittelt vielmehr der aufnehmenden Schule nur die Daten aus dem Schülerbogen, der Schülerakte und den sonstigen schriftlichen Nachweisen, die für den weiteren Bildungsgang des Schülers erforderlich sind. Krankheitsdaten zähle ich nicht zu den Daten, die „für den weiteren Bildungsgang“ des Schülers erforderlich sind.

Im Übrigen ist nach § 20 Abs. 4 Satz 2 Schulordnungsgesetz eine Unterrichtung der Schule über Gesundheitsdaten nur zulässig mit Einwilligung der Erziehungsberechtigten, sofern eine Information nicht aufgrund besonderer gesetzlicher Vorschriften zur Vorbereitung schulischer Entscheidungen erforderlich ist. Die fragliche Datenübermittlung hätte somit nicht ohne Einwilligung der Erziehungsberechtigten stattfinden dürfen.

Dem Anliegen der Petentin wurde letztlich dadurch Rechnung getragen, dass die Schule in dem neuen Bundesland die fraglichen Unterlagen vernichtet hat.

Darüber hinaus musste ich rügen, dass die alte Schule der Petentin keine Auskunft darüber geben konnte, welche Unterlagen an die neue Schule geschickt worden waren. Nach § 6 der oben genannten Verordnung haben die Erziehungsberechtigten ein Auskunftsrecht darüber, welche Daten an welche Stellen übermittelt worden sind. Ich habe die Schule darauf aufmerksam gemacht, dass in den Schülerunterlagen vermerkt werden muss, welche Informationen an welche Stellen weitergegeben worden sind.

13.2 Schüler- und Elterndaten am Schwarzen Brett

Durch eine Eingabe wurde ich darauf aufmerksam gemacht, dass am Schwarzen Brett eines Gymnasiums die Namen sämtlicher Schüler und Eltern mit Adresse, Telefonnummer, Handynummer und Konfessionszugehörigkeit ausgehängt waren. Besucher der Schule, Vertreter, Reinigungspersonal, Hausmeister konnten ebenso wie alle Schüler und Lehrer die Daten lesen. Datenschutzrechtlich war dies eine unzulässige Übermittlung personenbezogener Daten an Dritte.

Die Schulleitung erklärte, dass infolge einer Verwechslung die falsche Liste aufgehängt wurde. Der Fehler wurde sofort korrigiert.

13.3 Informationsrecht der Eltern volljähriger Schüler

Nach den Ereignissen an einer Schule in Erfurt – dort hatte ein Schüler in einem Amoklauf mehrere Mitschüler und Lehrer erschossen – ist eine bundesweite Diskussion darüber entbrannt, mit welchen Maßnahmen man künftig solche Geschehnisse möglichst verhindern könnte. Es wurde die Frage gestellt, ob nicht auch die mangelnde Information der Eltern des betroffenen Schülers durch die Schule eine Ursache gewesen sein könnte: Der Amokschütze war kurz vor der Tat von der Schule verwiesen worden, ohne dass die Eltern davon wussten.

Ein Blick in die datenschutzrechtlichen Vorschriften der Schulgesetze im Saarland zeigt, dass eine Unterrichtung der Eltern, etwa über den Leistungsstand oder schulordnungsrechtliche Maßnahmen, nicht mehr zulässig ist, sobald der Schüler das Volljährigkeitsalter erreicht hat. Gemäß § 36 Abs. 2 des Schulmitbestimmungsgesetzes ist den Erziehungsberechtigten der Leistungsstand ihres Kindes mitzuteilen sowie einzelne Beurteilungen zu erläutern. Der Gesetzgeber stellt somit für eine Informationsbefugnis eindeutig darauf ab, dass der Schüler noch minderjährig ist, denn nur insofern sind die Eltern erziehungsberechtigt.

Diese Regelung fügt sich ein in die bestehende Gesetzessystematik, wonach mit Vollendung des 18. Lebensjahres die elterliche Sorge und damit auch die gesetzliche Vertretung durch die Eltern enden.

Festzuhalten ist deshalb, dass aufgrund der derzeit bestehenden Rechtslage im Saarland eine Unterrichtung der Eltern volljähriger Schüler durch die Schule nicht zulässig wäre.

Sollte eine Gesetzesänderung erwogen werden, ist das Recht des volljährigen Schülers auf informationelle Selbstbestimmung als Konkretisierung seines allgemeinen Persönlichkeitsrechts aus Artikel 1 Abs. 1 und Artikel 2 Abs. 1 Grundgesetz zu beachten. Dieses gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen; Einschränkungen dieses Rechts sind im überwiegenden Allgemeininteresse hinzunehmen. Dabei muss der Einzelne vor unnötigen Eingriffen der öffentlichen Gewalt bewahrt bleiben; ein gesetzlicher Eingriff muss geeignet sein, das gesetzgeberische Ziel zu erreichen und darf den Einzelnen nicht übermäßig belasten.

Sollte sich der Gesetzgeber zu einer Gesetzesänderung entschließen, müsste er zunächst die Frage beantworten, inwiefern eine Information der Eltern geeignet sein könnte, Ereignisse wie die in Erfurt zukünftig zu vermeiden.

Ich möchte mich an dieser Stelle nicht von vornherein gegen eine entsprechende Gesetzesänderung aussprechen, meine aber, dass den Gesetzgeber eine Darlegungslast trifft, was die Frage der Geeignetheit betrifft.

Inhaltlich würde ich es begrüßen, wenn es keinen Automatismus bei entsprechenden Datenweitergaben gäbe, sondern differenzierte Entscheidungsmöglichkeiten der Schule im Einzelfall. Außerdem sollte möglichst eine Unterrichtung der betroffenen Schüler über die beabsichtigte Datenübermittlung erfolgen.

13.4 Verhaltenszeugnis der Sekundarstufe

Das Ministerium für Bildung, Kultur und Wissenschaft hatte im Jahre 2000 eine Verordnung über Verhaltenszeugnisse erlassen. Danach erhalten alle Schüler/innen der Sekundarstufe I, die die allgemeine Schulpflicht erfüllt haben, zusammen mit dem Abschluss- oder Abgangszeugnis ein Verhaltenszeugnis, in dem die Verhaltensmerkmale Betragen, Mitarbeit, Arbeitshaltung sowie Teamfähigkeit benotet werden. Das Zeugnis enthält außerdem entschuldigte und unentschuldigte Unterrichtsversäumnisse sowie Hinweise auf Tätigkeiten in der Schülervertretung und besondere außerschulische Aktivitäten. Mehrere Eltern und Elternvertreter hatten sich mit der Frage an mich gewandt, ob eine solche Regelung im Einklang mit den Grundsätzen des Datenschutzes stehe.

Das Oberverwaltungsgericht des Saarlandes hat nunmehr in seinem Urteil vom 19.08.2002 (Az. 3 N 1/01) zwar die Klageanträge von betroffenen Schülern zum überwiegenden Teil zurückgewiesen, die Verordnung in folgenden Punkten jedoch für nichtig erklärt:

- Ausweisung **entschuldigter** Unterrichtsversäumnisse, weil solche Angaben in einem Zeugnis, das typischerweise zur Verwendung bei Bewerbungen um einen Ausbildungsplatz dienen soll, einen Negativeffekt für das Schülerwohl haben könne, der nicht vom Unterrichts- und Erziehungsauftrag der Schule gedeckt sei.

- Ausweisung von Tätigkeiten in der **Schülervertretung**, weil (in Anlehnung an die Rechtsprechung über die Erwähnung einer Betriebsrats- oder Personalratstätigkeit im Arbeitszeugnis) dieses Engagement strikt neutral zu betrachten sei und zudem im Berufsleben keineswegs uneingeschränkte Befürwortung finde.

- Hinweise auf **außerschulische** Aktivitäten, weil für deren Aufnahme im Zeugnis das Schulordnungsgesetz keine Ermächtigungsgrundlage biete.

14 Öffentlicher Dienst

14.1 Nutzung von E-Mail und Internet am Arbeitsplatz

Immer mehr Bedienstete erhalten die Möglichkeit, an ihrem Arbeitsplatz das Internet zu nutzen und E-Mails zu verschicken und zu empfangen. In diesem Zusammenhang stellt sich zwangsläufig eine Vielzahl datenschutzrechtlicher Fragen, weil bei Nutzung dieser elektronischen Informations- und Kommunikationsdienste auch personenbezogene Daten gespeichert und genutzt werden müssen. Zu beantworten sind etwa Fragen wie: Welche Daten dürfen zu welchem Zweck gespeichert werden? Wer darf die Daten auswerten und unter welchen Voraussetzungen ist dies zulässig? Wann müssen die Daten wieder gelöscht werden? Eine Antwort auf diese Fragen findet sich in unterschiedlichen Gesetzen, wie z.B. dem Bundesdatenschutzgesetz bzw. den Landesdatenschutzgesetzen, im Telekommunikationsgesetz, in der Telekommunikationsdatenschutzverordnung oder im Teledienstedatenschutzgesetz. Je nachdem, ob nur die dienstliche oder auch die private Nutzung erlaubt ist, wird die Antwort unterschiedlich ausfallen, da der Arbeitgeber bei Erlaubnis der privaten Nutzung stärkeren Restriktionen unterworfen ist. Wegen der Unübersichtlichkeit der Materie und weil hier schwierige Rechtsfragen zu entscheiden sind, für die es noch kaum Rechtsprechung gibt, haben sich der Bundesbeauftragte und die Landesbeauftragten für den Datenschutz entschlossen, in einer „Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz“ eine Hilfestellung zu geben. Zusätzlich haben die Datenschutzbeauftragten in einer Entschließung (siehe Anlage 13) ihre grundlegenden Positionen zu diesem Thema zusammengefasst.

Der Text der Orientierungshilfe ist in unserem Internet-Angebot unter www.lfd.saarland.de abrufbar.

14.2 Neue Telekommunikations-Richtlinien

Das Ministerium für Finanzen und Bundesangelegenheiten hat – insbesondere wegen der zunehmenden Verbreitung des Mobilfunks - die "Richtlinien über die Einrichtung und Nutzung der dienstlichen Fernmelde- und Telekommunikationsanlagen einschließlich der Kostenregelung (TK-Richtlinien)" aus dem Jahre 1989 überarbeitet; die Neufassung ist am 01.10.2002 in Kraft getreten.

Beim Einsatz von Mobilfunkgeräten für dienstliche Zwecke wird stets ein Einzelverbindungsnachweis angefordert, aus dem hervorgeht, mit welcher Zielrufnummer, wann, wie lange telefoniert wurde. Auf mein Verlangen wird bei Beschäftigten, die nach § 203 Abs. 1 StGB einem besonderen Berufsgeheimnis unterliegen (z.B. Betriebsarzt, Psychologe oder Sozialarbeiter in der Sucht- und Sozialberatung), kein Einzelverbindungsnachweis erstellt, damit die Identität des angerufenen Klienten nicht preisgegeben wird. Bei den übrigen Beschäftigten sind die Nachweise – wie die Ausdrucke über Dienstgespräche im Festnetz – nach der Auswertung, spätestens zwei Monate nach Ablauf des Abrechnungszeitraums, zu vernichten.

Bei Privatgesprächen wird die Zielrufnummer (entsprechend § 7 Abs. 3 Telekommunikations-Datenschutzverordnung) nun verkürzt um die drei letzten Ziffern (bisher zwei) erfasst.

14.3 Handlungsempfehlungen zur Verbesserung der Anwesenheitszeiten

Aufgrund eines Hinweises der Personalvertretung habe ich mich mit den vom Ministerium für Inneres und Sport herausgegebenen "Handlungsempfehlungen zur Verbesserung der Anwesenheitszeiten" befasst. Diese Anleitung, in der Maßnahmen zur Senkung der Krankheitsquote in der Landesverwaltung empfohlen werden, enthält Formulierungen, die unter Datenschutzgesichtspunkten problematisch sind.

In der Diskussion mit dem Ministerium konnten folgende Klarstellungen erzielt werden:

- In den Dienstbesprechungen der Führungskräfte der Dienststelle („Leitungsbesprechungen“) werden keine Krankenstände einzelner Mitarbeiter und Mitarbeiterinnen erörtert.
- Die Personalverwaltung stellt den unmittelbaren Vorgesetzten keine Übersicht über die Abwesenheitstage der Bediensteten ihrer Organisationseinheit zur Verfügung.
- Fehlzeitengespräche werden von der Personalverwaltung geführt. Es ist nicht Aufgabe des unmittelbaren Vorgesetzten, die Ursachen der Erkrankung einzelner Mitarbeiter und Mitarbeiterinnen zu erforschen.
- Bei den Rückkehrgesprächen werden keine Fragen über die Art der jeweiligen Erkrankung gestellt.

Die durch verschiedene Formulierungen der Empfehlungen entstandenen Missverständnisse sind offenbar noch nicht ausgeräumt. Ein Ressort beabsichtigte, zum Vollzug der Handlungsempfehlungen den Abteilungen halbjährlich die Fehlzeiten der einzelnen Mitarbeiterinnen und Mitarbeiter, aufgeschlüsselt nach der Anzahl der Krankmeldungen und der Dauer der Erkrankung mitzuteilen. Ich habe dem Ministerium von dieser routinemäßigen Übermittlung abgeraten.

14.4 Einsichtnahme in die Personalakte

In der Personalabteilung einer Gemeinde erschien ein Mitglied des Gemeinderates in Begleitung seiner bei der Kommune beschäftigten Nichte und verlangte Einsicht in deren Personalakte. Die Einsichtnahme wurde der Angestellten und dem Onkel mit dem Hinweis verwehrt, eine solche Maßnahme sei über den Bürgermeister zu beantragen, der auch den Zeitpunkt und den Ort der Akteneinsicht festsetze. Das Angebot, sofort mit dem Bürgermeister zu reden, nahmen beide nicht an.

Ich habe dem Bürgermeister, der mich um eine Stellungnahme zu dem Vorfall bat, mitgeteilt, dass die Gemeindebeschäftigten grundsätzlich ein Recht auf Einsicht in ihre Personalakte haben. Die Geltendmachung dieses aus dem Fürsorgeprinzip abgeleiteten Rechts darf nicht von einer bestimmten Form, z.B. der Schriftform oder der Verwendung eines bestimmten Antragsformulars abhängig gemacht werden. Das Verlangen der Personalabteilung, die Einsicht "über den Bürgermeister zu beantragen", hielt ich für eine unnötige Erschwerung des Einsichtsrechts. Die Personalverwaltung hat Ort und Zeitpunkt der Einsichtnahme nach pflichtgemäßem Ermessen zu konkretisieren. Dabei ist insbesondere die dienstliche Beanspruchung und Terminplanung der Aufsichtsperson zu berücksichtigen, weil die Einsichtnahme nur im Beisein eines Mitarbeiters der Personalverwaltung erfolgen sollte, um Manipulationsmöglichkeiten an der Personalakte auszuschließen. Der Darstellung des Vorgangs waren keine Anhaltspunkte zu entnehmen, die einer unverzüglichen Gewährung der Einsicht im Wege gestanden hätten.

Sowohl beamtenrechtliche als auch tarifvertragsrechtliche Regelungen erlauben dem Beschäftigten, sich bei der Einsicht durch einen Bevollmächtigten vertreten zu lassen, soweit (im Ausnahmefall) dienstliche Gründe nicht entgegenstehen. Sofern keine schriftliche Vollmacht vorgelegt wird, sollte die Personalverwaltung zumindest die Umstände der Bevollmächtigung dokumentieren. Ob es sich im vorliegenden Fall des Onkels und Gemeinderatsmitglieds um eine solche Bevollmächtigung handelte, hätte durch Befragen der Angestellten geklärt werden können. In seiner Funktion als Gemeinderatsmitglied durfte der Onkel jedenfalls keine Akteneinsicht nehmen. Die Voraussetzungen des § 37 Kommunalselbstverwaltungsgesetz, der die Informationsrechte des Gemeinderates im Einzelnen regelt, waren offensichtlich nicht erfüllt.

14.5 Information des Gemeinderates über Nebentätigkeiten von Gemeindebediensteten

Ein Problem, das in den Kommunen immer wieder auftaucht, ist die Frage, in welchem Umfang der Gemeinderat Informationen über personenbezogene Sachverhalte von der Gemeindeverwaltung beanspruchen kann.

Antwort auf diese Frage gibt § 37 des Kommunalselbstverwaltungsgesetzes. Gemäß § 37 Abs. 1 Satz 2 dieser Vorschrift können sich die Mitglieder des Gemeinderates von der Bürgermeisterin oder vom Bürgermeister über alle Angelegenheiten, die der Beschlussfassung des Gemeinderates, seiner Ausschüsse oder eines Bezirksrates oder Ortsrates unterliegen, unterrichten lassen. Zur Wahrnehmung dieser Rechte dürfen dem Gemeinderat personenbezogene Daten im jeweils erforderlichen Umfang übermittelt werden (§ 37 Abs. 2 KSVG). Diese Regelungen im Gemeinderecht sind spezialgesetzliche Ausprägungen des im Datenschutzrecht allgemein geltenden Grundsatzes, wonach jede Stelle über diejenigen Daten verfügen darf, die sie zur Erfüllung ihrer Aufgaben benötigt.

In konkreten Fällen musste ich mich mit der Frage befassen, ob es datenschutzrechtlich zulässig ist, den Gemeinderat darüber zu informieren, welche Nebentätigkeiten von den einzelnen Gemeindebediensteten ausgeübt werden. In den zugrunde liegenden Fällen hatten Gemeinderatsfraktionen den Bürgermeister um entsprechende Auskünfte gebeten.

Die befragten Bürgermeister hatten es jeweils unter Berufung auf die Datenschutzrechte der Bediensteten abgelehnt, die verlangten Informationen zu erteilen.

Dieser datenschutzrechtlichen Bewertung konnte ich mich in vollem Umfang anschließen. Denn wie oben ausgeführt, besteht eine Unterrichtungspflicht des Bürgermeisters lediglich hinsichtlich solcher Angelegenheiten, die der Beschlussfassung des Gemeinderates unterliegen. Hierzu gehört die Erteilung von Nebentätigkeitsgenehmigungen aber eindeutig nicht. Zuständig für die Erteilung von Nebentätigkeitsgenehmigungen an Gemeindebedienstete ist vielmehr die Bürgermeisterin oder der Bürgermeister als oberste Dienstbehörde (§ 80 Abs. 5 Satz 1 Saarländisches Beamtengesetz in Verbindung mit § 59 Abs. 5 KSVG).

Keine datenschutzrechtlichen Bedenken bestehen gegen die allgemeine Auskunft, dass Nebentätigkeitsgenehmigungen an Gemeindebedienstete erteilt worden sind, sofern diese keine Rückschlüsse auf bestimmte Personen ermöglicht.

Die geschilderten Beispielsfälle machen deutlich, dass auch innerhalb einer Gemeinde ein unbeschränkter Informationsaustausch nicht statthaft ist.

14.6 Personaldaten im freien Zugriff

Ein Beamter des Ministeriums für Umwelt stellte an seinem Arbeitsplatz-PC zufälligerweise fest, dass ein ihn betreffendes Schreiben der Personalabteilung auf einem für alle Mitarbeiter der Behörde zugänglichen Bereich des Servers gespeichert war. Es handelte sich um einen Schriftsatz an das Verwaltungsgericht in einem Rechtsstreit, den der Betroffene mit seinem Dienstherrn führte. Das Ministerium räumte ein, dass aufgrund eines "Büroversehens" tatsächlich der Entwurf des Schriftsatzes in einem "allgemein zugänglichen Verzeichnis" gespeichert wurde. Die Informationen waren dort mehrere Monate verfügbar; sie wurden erst nach der Beschwerde des Beamten entfernt. Dem Wunsch des Betroffenen, einen Schadenersatzanspruch festzustellen, konnte ich wegen fehlender gesetzlicher Befugnis nicht entsprechen. Einen solchen Anspruch muss er – eventuell auf dem Rechtswege – selbst geltend machen.

14.7 Organisation der Personalaktenführung bei einem Landesbetrieb

Bei der Prüfung eines Landesbetriebs habe ich vorgeschlagen, die Zuständigkeit für die Personalaktenführung zu ändern. Während die Führung der Personalakten der Beamten und Angestellten beim Ministerium liegt, sollten die Personalakten der Arbeiter dezentral auf die Einsatzorte aufgeteilt werden. Zudem wurden Personalnebenakten für Beamte und Angestellte am jeweiligen Einsatzort sowie weitere Personalunterlagen in der Personalabteilung des Landesbetriebs vorgehalten. Nachdem der Landesbetrieb eine spezielle Organisationseinheit für Personalangelegenheiten eingerichtet hat, sollten aus Gründen des Personaldatenschutzes klare Verhältnisse geschaffen und alle Personalakten (Personalakten der Arbeiter, Personalnebenakten der Beamten und Angestellten) ausschließlich bei dieser Stelle geführt werden. Die Personalnebenakten sind zudem auf den für die Aufgabenerfüllung vor Ort erforderlichen Umfang zu reduzieren. Der Landesbetrieb hat zugesichert, künftig so zu verfahren.

Auch die Aufbewahrung der Personalunterlagen war unzulänglich. Zum Zeitpunkt der Prüfung waren Personalakten u.a. außerhalb der Personalabteilung in einem Schrank gelagert, der nicht ausreichend gesichert war. Jedenfalls wurde kurz zuvor eine in diesem Schrank aufbewahrte Personalakte infolge ungeklärter Umstände im Papierabfall aufgefunden. Inzwischen wurde für die Personalabteilung ein Stahlschrank beschafft, in dem die Personalakten aufbewahrt werden.

Außerdem gab es Mängel bei der Schriftgutentsorgung. Obwohl ein Reißwolf der Sicherheitsstufe 4 zur Verfügung steht, wurden – wie ich bei meinem (angekündigten!) Kontrollbesuch feststellte – stoßweise Unterlagen mit personenbezogenen Daten im allgemein zugänglichen Papierabfallbehälter abgelegt. Der Landesbetrieb hat zugesagt, durch organisatorische Maßnahmen sicherzustellen, dass diese Art der Schriftgutentsorgung künftig unterbleibt.

14.8 Personalservice-Center, Personalbörse

Beim Chef der Staatskanzlei wird ein Personalservice-Center eingerichtet, das vor allem folgende Aufgaben hat:

- Vermittlung von Landesbediensteten (insbesondere veränderungswillige Mitarbeiterinnen und Mitarbeiter, nur noch eingeschränkt Dienstfähige sowie solche Beschäftigte, deren Tätigkeiten durch Strukturmaßnahmen wegfallen) auf freie Dienstposten innerhalb und außerhalb der Landesverwaltung;
- Koordinierungsstelle für die Vermittlung von Beschäftigten von und zu anderen öffentlichen oder privaten Arbeitgebern;
- Förderung der Mobilität und Verwendungsbreite von Beschäftigten;
- Qualifizierung von Beschäftigten, die in der Personalbörse geführt werden.

Für diese Zwecke wird eine "Personalentwicklungsdatenbank" eingesetzt, in der u.a. Daten über Ausbildung, Kenntnisse und Befähigungen, derzeitige Arbeitsplatzsituation und Verwendungswunsch des Beschäftigten gespeichert werden.

Bei den Besprechungen mit der Staatskanzlei bestand Einvernehmen, dass nur solche Bediensteten in der Datenbank erfasst werden, die ausdrücklich hierzu ihre Einwilligung erteilt haben. Eine gesetzliche Befugnis, die es den Ressorts erlaubt, dem Personalservice-Center Daten ohne Einwilligung der Betroffenen zu übermitteln, besteht nicht. Meine Vorschläge zur Gestaltung des Verfahrens und zur Beschränkung des Datenbankinhalts wurden weitgehend berücksichtigt. Nicht übernommen wurde meine Empfehlung, den Beschäftigten, die sich um eine andere Stelle in der Landesverwaltung bewerben, freizustellen, ob sie das Bewerbungsschreiben auf dem Dienstweg an die Personalbörse weiterleiten. Ich halte es nicht für notwendig, dass der Beschäftigte seinen Veränderungswunsch bereits zum Zeitpunkt der Bewerbung dem Vorgesetzten offenbaren muss.

14.9 Vorlage des amtsärztlichen Zeugnisses für die Urlaubsgewährung bei einer Kur

Ein Beamter der Landesverwaltung hat sich mit einer Eingabe an mich gewandt, weil seine Dienstbehörde für die Bewilligung des "Sonderurlaubs" bei einer Kur das amtsärztliche Zeugnis verlangt, das die Notwendigkeit der Kur begründet und das daher auch die medizinischen Diagnosen enthält. Er ist wie ich der Meinung, dass es die Dienststelle oder die Personalverwaltung nicht zu interessieren hat, wegen welcher Krankheiten ihm die Kur genehmigt wurde.

Nach § 10 UrlaubsVO wird Urlaub für eine Heilkur, deren Notwendigkeit durch ein amts- oder vertrauensärztliches Zeugnis nachgewiesen ist, nicht auf den Erholungsurlaub angerechnet. Diese Vorschrift erfordert meines Erachtens nicht, dass das ärztliche Zeugnis der Dienstbehörde für die Bewilligung des "Sonderurlaubs" vorgelegt wird, sondern setzt lediglich voraus, dass der Genehmigung der Kur ein amts- oder vertrauensärztliches Zeugnis zugrunde liegt. Das Vorliegen dieser Voraussetzung wird in der Anerkennung der Beihilfefähigkeit der Kur durch die Zentrale Beihilfestelle beim Landesamt für Finanzen (oder einer anderen Beihilfefestsetzungsstelle) ausdrücklich bestätigt. Ich halte es daher für ausreichend, wenn der Beamte seinem Urlaubsantrag eine Kopie der Anerkennung beifügt. So wird es nach meiner Kenntnis in den meisten Behörden gehandhabt.

Das Ministerium für Inneres und Sport, das ich zu dieser Frage um Stellungnahme bat, hält den Dienstherrn demgegenüber für berechtigt, das amtsärztliche Zeugnis zu verlangen. Dieses Gutachten dürfe "aus Gründen des Datenschutzes jedoch nur über die Notwendigkeit der Heilkur Zeugnis ablegen, indes nicht über die der Feststellung zugrunde liegenden medizinischen Befunde". Da das amtsärztliche Zeugnis notwendigerweise stets die medizinischen Diagnosen enthält, ist die Frage noch immer nicht geklärt, wie der Beamte den Nachweis für die Bewilligung des Urlaubs zu führen hat. Ich habe dem Ministerium vorgeschlagen, dass der Amtsarzt bei der Ausstellung des Gutachtens ein Duplikat unter Weglassen der Krankheitsbezeichnungen ausdruckt. Die Zentrale Gutachtenstelle für Landesbedienstete sollte beauftragt werden, das Amtsärztliche Zeugnis zum Antrag auf Anerkennung der Beihilfefähigkeit von Kosten für eine Heilkur oder einen Sanatoriumsaufenthalt in dieser Form auszustellen. Ein nennenswerter Mehraufwand entsteht durch eine solche Verfahrensweise beim Einsatz eines Textverarbeitungssystems, wie er auch bei der Gutachtenstelle üblich ist, nicht.

Wie mein Vorschlag realisiert wird, war bei Redaktionsschluss noch nicht bekannt. Ich gehe jedoch davon aus, dass er entsprechend umgesetzt wird.

15 Rundfunk und Medien, Telekommunikation

15.1 Saarländisches Mediengesetz

Im Berichtszeitraum hatte ich Gelegenheit, zu dem Entwurf eines Saarländischen Mediengesetzes aus datenschutzrechtlicher Sicht Stellung zu nehmen.

Ziel des Gesetzes sollte die Schaffung eines einheitlichen Ordnungsrahmens für alle Medien sein, der die bisherigen unterschiedlichen gesetzlichen Regelungen im Pressegesetz und Rundfunkgesetz ablöst. Zentrale Aspekte des Gesetzes sind nach Presseverlautbarungen der Landesregierung die Stärkung der Selbstkontrolle und Selbstregulierung der Medien und Medienaufsichtsbehörden, die Umsetzung von Deregulierung und Privatisierung sowie die Stärkung der aktiven Bürgergesellschaft auch im Bereich der Medien, die Entwicklung der Informationsgesellschaft im Saarland und die Neuausrichtung der Tätigkeit der Landesmedienanstalt für das Saarland.

Die Absicht, den Ordnungsrahmen in einem einzelnen Gesetz zusammenzufassen, habe ich grundsätzlich begrüßt, weil dies geeignet sein kann, die Transparenz der Regelung zu verbessern. Ich habe allerdings Zweifel angemeldet, ob dieses Ziel im Bezug auf den Datenschutz erreicht wird, wenn das zusammenfassende Gesetz seinerseits auf unterschiedliche Regelungswerke verweist.

Vor allen Dingen hatte ich mir inhaltlich ein Mehr an Datenschutz vorgestellt. So habe ich in meiner Stellungnahme darauf hingewiesen, dass der Entwurf meines Erachtens nicht in ausreichendem Umfang der Verpflichtung durch die EG-Datenschutzrichtlinie nachkommt, das Recht auf informationelle Selbstbestimmung effektiver als bisher zu schützen.

Für den Datenschutz bei Presseunternehmen sollte es bei einem bloßen Zitat der rahmenrechtlichen Regelung entsprechend § 41 BDSG verbleiben. Ich habe die Auffassung vertreten, dass unabhängig von der Frage, ob die inhaltlichen Vorgaben des Rahmenrechts als solche für das Bundesrecht ausreichen, der Landesgesetzgeber seine Verpflichtung zur Umsetzung der EG-Datenschutzrichtlinie mit einer solchen Regelung nicht ausreichend nachkomme. Es bedürfe vielmehr sowohl einer Abwägung der Interessen mit dem Ziel, von der grundsätzlich bestimmten Verbesserung des Datenschutzes die Medien nur insoweit auszunehmen, als „sich dies als notwendig erweist, um das Recht der Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen“ (Erwägungsgrund [17] der Richtlinie), als auch eines geeigneten Instrumentariums zu dessen Durchsetzung.

Zwar kommen als Steuerungsmittel nicht notwendigerweise allein staatliche Rechtsnormen in Betracht. Die freiwillige Selbstkontrolle durch den Deutschen Presserat, auf die der Bundesgesetzgeber seinen Verzicht auf eingehende Rahmenregelungen gegründet hat, lässt auch durchaus positive Grundsätze und Verfahren erkennen, die mir und meinen Kollegen zwischenzeitlich näher erläutert wurden. Ihre Durchsetzung kann aber staatlicherseits nicht gewährleistet werden, und sie greifen von vornherein nicht bei solchen Presseunternehmen, die nicht in den Trägerorganisationen des Presserates zusammengeschlossen sind. Sie unterliegen auch keinerlei inhaltlicher Prüfung oder Gewährleistung durch die Länder, die doch bundesrechtlich ausdrücklich verpflichtet werden, in ihrer Gesetzgebung die Anwendung des Schutzes vorzusehen; die Bestimmungen des Presserates über die Selbstkontrolle sind – auch nach dessen eigener Vorstellung – keine Verhaltensregeln im Sinne des § 38 BDSG und ganz bewusst nicht den Aufsichtsbehörden zur Kontrolle vorgelegt worden. Inhaltlich erscheint im Übrigen fraglich, ob ein Verfahren ausreichenden Schutz gewährt, das bei einem Verstoß die Überprüfung und gegebenenfalls Sanktion allein durch Vertreter der Medien vorsieht, nicht aber eine Mitwirkung betroffener oder sonstiger dritter Stellen.

Insoweit verbleibt bei einem Verzicht des Landesgesetzgebers auf jegliche materielle Ausfüllung der Rahmenvorschrift die Möglichkeit eines Verstoßes sowohl gegen die Vorgabe der EG-Datenschutzrichtlinie, durchgehend ein ausreichendes Datenschutzniveau zu schaffen, als auch gegen die bundesrechtliche Verpflichtung der Länder, diesen Schutz „in ihrer Gesetzgebung“ vorzusehen.

Darüber hinaus habe ich auch angemerkt, dass die jeweiligen Ordnungsrahmen für Presseunternehmen und Rundfunkveranstalter materiell erheblich unterschiedlich ausgestaltet sind. Die Unterschiede wirken sich auch auf inhaltlich übereinstimmende Medieninhalte aus, wenn solche sowohl in der Presse als auch im Rundfunk verbreitet werden, wie dies bei Nutzung beider Formen zunehmend der Fall ist.

Das Saarländische Mediengesetz ist zwischenzeitlich in Kraft getreten, ohne dass meine im Gesetzgebungsverfahren geäußerten Bedenken aufgegriffen wurden. Es bleibt abzuwarten, wie sich das Instrument der freiwilligen Selbstkontrolle durch den Deutschen Presserat in der Praxis bewährt.

15.2 Neue Medienordnung

Bund und Länder haben damit begonnen, über die Grundzüge einer neuen Medienordnung zu verhandeln.

Dabei wird auch darüber diskutiert, die materiellen Regelungen zum Datenschutz im Bereich der elektronischen Medien (Teledienste, Mediendienste, Rundfunk) zusammenzufassen. Ein weiterer Gesichtpunkt ist die Notwendigkeit einer Veränderung der bestehenden Aufsichtsstrukturen für den elektronischen Mediendatenschutz.

Die Datenschutzbeauftragten von Bund und Ländern haben in einer Entschließung vom 25./26. Oktober 2001 (Anlage 14) die Notwendigkeit betont, auch bei einer veränderten Ordnung tragende Grundrechte unserer Verfassung durchgängig zu gewährleisten.

15.3 Datenschutz in der Telekommunikation und im Internet

Die Sorge um das Recht auf informationelle Selbstbestimmung sowohl auf nationaler als auch auf internationaler Ebene bei der Nutzung moderner Medien hat die Datenschutzbeauftragten des Bundes und der Länder zu mehrfachen Appellen an den Gesetzgeber veranlasst, auch in diesem Zusammenhang das rechte Augenmaß für einen Ausgleich zwischen der allgemeinen Straftatenbekämpfung, dem berechtigten Strafverfolgungsinteresse und dem Grundrecht auf Datenschutz zu wahren (Anlagen 15, 16, 17 und 18)

Die Datenschutzbeauftragten wenden sich insbesondere gegen die lückenlose Registrierung des Nutzerverhaltens, da Kriminelle in der Lage sind, solche Hürden zu umschiffen und damit zu erwarten ist, dass dann die Daten aller Unbeteiligten, die sich rechtmäßig verhalten, übrig bleiben und auf Vorrat gespeichert würden.

Bevor man solche Wege der Registrierung aller Mediennutzer bei den Betreibern beschreitet, wäre die Sinnhaftigkeit und Angemessenheit in der Öffentlichkeit ausführlich zu diskutieren. Vor allem sind bereits vorhandene Instrumente durch eine unabhängige Stelle zu evaluieren, denn der Gesetzgeber hat in jüngster Zeit zahlreiche neue Befugnisse für die Sicherheitsbehörden geschaffen, deren Kumulation zukünftig ohnehin zu einer verstärkten Einbeziehung Unbeteiligter in staatliche Maßnahmen führen wird.

16 Sonstiges

16.1 Bloßstellung Betroffener durch unvollständige Adressierung

Als einer der großen Arbeitgeber im Saarland ist der Saarländische Rundfunk und dessen eigener Datenschutzbeauftragter auf ein Problem gestoßen, das die Datenschutzbeauftragten anderer öffentlicher Stellen und auch mich über die Jahre hinweg beschäftigt hat und in Einzelfällen leider immer noch beschäftigt.

Grund des Anstoßes ist die wenig sensible Adressierung durch öffentliche Stellen, insbesondere Justizbehörden, die es versäumen, in Personalangelegenheiten gleich die Personalabteilung anzuschreiben und etwa durch den Zusatz „Vertraulich“ kenntlich zu machen, dass erst dort die Post geöffnet werden darf.

Diesen allgemeinen Missstand habe ich aufgrund der Anregung des Datenschutzbeauftragten des Saarländischen Rundfunks auch gern zum Anlass genommen, in einer Pressemitteilung eine sorgfältigere Adressierung durch verantwortliche Stellen anzumahnen.

So muss beispielsweise ausgeschlossen werden, dass Pfändungs- und Überweisungsbeschlüsse der Gerichte und entsprechende Verfügungen öffentlicher Stellen zunächst wegen fehlender exakter Adressierung von der Poststelle durch das jeweilige Haus irren, bis sie die Personalstelle erreicht haben. Auf diesem Wege kommen finanzielle Schwierigkeiten der Betroffenen etlichen unzuständigen Personen zu Gesicht. Auch in Scheidungsangelegenheiten ist eine mangelhafte Adressierung, die zur Kenntnisnahme von sensiblen Daten durch nicht zuständige Personen führt, besonders peinlich.

Als angemessene Vorkehrung könnte hier ein kleiner Zusatz im Brieffenster, wie z.B. „Personalabteilung“, „Personalbereich“ oder „Personalsache/Versorgung“ verbunden mit dem Wort „Vertraulich“ Abhilfe schaffen. Damit erreicht der ungeöffnete Brief ausschließlich den funktionell zuständigen Bediensteten. So ist es im Justizmitteilungsgesetz und den dazu ergangenen Anordnungen in Zivilsachen und Strafsachen zum Schutze dieser Daten bereits vorgesehen.

Die gesetzlichen Vorgaben nützen allerdings wenig, wenn der Absender für die Belange des Betroffenen in der Praxis kein Gespür entwickelt. Jeder Absender sollte daher bedenken, dass sein Arbeitgeber morgen der Adressat einer Mitteilung über ihn sein könnte.

Aufgrund der Unterstützung durch den Datenschutzbeauftragten des Saarländischen Rundfunks, dem ich an dieser Stelle für eine gute Zusammenarbeit danke, haben meine Hinweise auch eine verstärkte Verbreitung gefunden. In Zukunft ist immer wieder an diese Grundsätze zu erinnern, da sie nur allzu rasch in Vergessenheit geraten.

16.2 Urheberrecht in der Informationsgesellschaft

Vorgaben in der EU-Urheberrechtsrichtlinie haben den Gesetzgeber zu neuen Planungen für Regelungen im Urheberrecht veranlasst. Zur Abgeltung der Vergütungsansprüche der Urheberinnen und Urheber, die bisher durch ein System der Pauschalabgaben auf Geräte und Kopiermedien befriedigt wurden, sollte eine vorrangige individuelle Lizenzierung in Erwägung gezogen werden, die allerdings auch zur individuellen Erstellung von Nutzungsprofilen führen würde.

Die Datenschutzbeauftragten des Bundes und der Länder haben dazu in einer Entschließung auf die Rechtsprechung des Bundesgerichtshofes hingewiesen, der eine solche Verfahrensweise beim Einsatz analoger Kopiertechnik nicht in Einklang mit dem verfassungsrechtlichen Schutz der persönlichen Freiheitsrechte der Nutzerinnen und Nutzer bezeichnet hat (Anlage 19).

Diese Kriterien sind auch auf die digitale Verwaltung digitaler Rechte zu übertragen.

16.3 Elektronisches Fahrgeldmanagement

Auf kommunaler Ebene sind auch im Saarland Verkehrsbetriebe vorhanden, die als öffentliche Stellen im Sinne des Datenschutzrechts anzusehen sind und damit auch meiner Kontrollkompetenz unterliegen.

Die maßgeblich von meiner nordrhein-westfälischen Kollegin in Zusammenarbeit mit dem Verband der deutschen Verkehrsunternehmen erstellten Grundanforderungen für ein elektronisches Fahrgeldmanagement können für diese Stellen Richtschnur für ein datenschutzgerechtes Verfahren bei der Einführung und der Verwaltung eines elektronischen Fahrgeldmanagements sein, das die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in dieser Form zustimmend zur Kenntnis genommen hat (Anlage 20).

16.4 Neues Abrufverfahren bei den Kreditinstituten

Manche Gesetzesänderung findet nicht die Beachtung in der Öffentlichkeit, die sie eigentlich verdient hätte. So sollten Bankkunden darüber informiert sein, dass die zuständige Bundesanstalt nach dem Vierten Finanzmarktförderungsgesetz, das Mitte 2002 veröffentlicht wurde, die von den Kreditinstituten vorzuhaltenden Daten, wer welche Konten und Depots hat, ohne Kenntnis der Kundinnen und Kunden zur eigenen Aufgabenerfüllung oder zu Gunsten anderer öffentlicher Stellen abrufen kann. In einer Entschließung haben die Datenschutzbeauftragten des Bundes und der Länder betont, dass dieser neue Eingriff in die Vertraulichkeit der Bankbeziehung durch die Kreditinstitute transparent gemacht werden soll. Ebenso wäre auf die Erweiterung der Pflichten der Kreditinstitute zu einer intensiveren Kontenüberwachung nach dem so genannten „know your customer principle“ aufmerksam zu machen (Anlage 21).

In meinem Zuständigkeitsbereich sind hier die Sparkassen besonders anzusprechen, bei denen uns in einem Einzelfall die verstärkten Pflichten zur Kontenüberwachung beschäftigt haben.

Die betroffene Sparkasse hat nach den rechtlichen Bestimmungen völlig korrekt gehandelt, der Kunde war allerdings über die Änderung eines jahrelangen – bis dato problemlosen – Verfahrens befremdet. Wenn er über den Grund der Verfahrensänderung aufgeklärt worden wäre, so seine Einlassung, hätte er sich auch williger an einem neuen, reibungslosen Verfahren beteiligen wollen.

16.5 Fördermitteldatenbank bei der Staatskanzlei

Im Berichtszeitraum wurde mir der Entwurf eines „Gesetzes über die Einrichtung einer elektronischen Fördermitteldatenbank im Saarland“ zur Stellungnahme aus datenschutzrechtlicher Sicht vorgelegt.

In dieser Datenbank, die bei der Staatskanzlei geführt werden soll, sollen alle Anträge auf Fördermittel aus dem Landeshaushalt gespeichert werden. Die Aufgaben der elektronischen Fördermitteldatenbank werden laut Gesetzesbegründung darin bestehen, „das Controlling und die laufende Analyse der Förderpraxis sicherzustellen sowie die Ausübung der Rechts- und Fachaufsicht und die Information über sämtliche Fördermaßnahmen des Landes zu unterstützen.“

Antragsteller auf Fördermittel werden meist juristische Personen des Privat- und öffentlichen Rechts sein, es gibt jedoch auch Fördermittel, die von natürlichen Personen beantragt werden können, so dass deren informationelles Selbstbestimmungsrecht tangiert ist.

Die Notwendigkeit einer speziellen gesetzlichen Regelung für die Errichtung einer landeseinheitlichen Fördermitteldatenbank ist insbesondere unter dem Gesichtpunkt begründet, dass personenbezogene Daten durch eine Stelle verarbeitet werden sollen, die für die eigentliche Fördermittelverwaltung und Antragsbearbeitung nicht zuständig ist. (Die Anträge auf Bewilligung von Fördermitteln werden nicht in der Staatskanzlei, sondern in den Geschäftsbereichen der einzelnen Ministerien bearbeitet. Die Bearbeitung der konkreten Fördervorhaben erfolgt nach spezialrechtlichen Regelungen. Art und Umfang der Verarbeitung der hierfür erforderlichen personenbezogenen Daten richtet nach diesen Rechtsgrundlagen bzw. nach dem Saarländischen Datenschutzgesetz, ihre Verarbeitung ist nicht Gegenstand des zur Diskussion stehenden Gesetzentwurfes.)

Ich begrüße es ausdrücklich, dass dieser Regelungsbedarf von der Staatskanzlei von vornherein gesehen wurde und offensichtlich nicht daran gedacht war, eine solche Datenbank ohne entsprechende gesetzliche Grundlage zu schaffen.

Einige Änderungsvorschläge, die ich zu Detailfragen gemacht hatte, wurden von der Staatskanzlei, deren konstruktiv kooperative Haltung als absolut erfreulich zu bezeichnen ist, aufgegriffen.

Ich gehe davon aus, dass die Zusammenarbeit bei der nach dem Gesetzentwurf zu erlassenden Rechtsverordnung, in der Inhalt und Umfang der zu verarbeitenden Daten sowie deren Löschung zu regeln ist, ebenso konstruktiv sein wird.

16.6 Nutzung von Beständen des Landesarchivs (Geschichte der saarländischen Anwaltschaft)

Das Ministerium der Justiz hat mich zu folgendem Sachverhalt um eine datenschutzrechtliche Stellungnahme gebeten:

Der saarländische Anwaltverein hatte die Idee, die Geschichte der Rechtsanwälte im Saarland von 1835 bis 1960, also von der Gründung des Landgerichts Saarbrücken bis zum Abschluss der Wiedereingliederung des Saarlandes in die BRD zu erforschen. Dem Anwaltverein ging es darum, Rückschlüsse zur Organisation und Tätigkeit der Anwaltschaft, aber auch biografische Daten zu einzelnen Anwälten und Anwältinnen darzustellen. Mit der Erstellung der Studie wurde ein Historiker beauftragt, der zu diesem Zweck Einsicht in die beim saarländischen Landesarchiv befindlichen Personalakten von saarländischen Anwälten und Anwältinnen nehmen wollte. Dem Historiker ging es darum, aus diesen Akten ein „Soziogramm“ der saarländischen Anwaltschaft im Lauf von mehr als 100 Jahren zu erstellen (familiäre Herkunft, soziales Milieu, bevorzugte Studienorte, Heirat und Herkunft des Ehepartners, Kinder usw.) Außerdem sollten die Lebensläufe in Form von Kurzbiografien als Anhang des Buches veröffentlicht werden. Veröffentlicht werden sollten solche Daten wie z.B. Studium, Zulassung oder Löschung an Amtsgerichten und am Landgericht Saarbrücken.

Die Nutzung von im saarländischen Landesarchiv archivierten personenbezogenen Unterlagen ist im saarländischen Archivgesetz vom 23. September 1992 (Amtsblatt 1992, S. 1094) geregelt. Zum Schutz der Persönlichkeitsrechte legt das saarländische Archivgesetz Schutzfristen fest, vor deren Ablauf personenbezogenes Archivgut grundsätzlich nicht genutzt werden darf. Diese Schutzfrist endet 30 Jahre nach dem Tode; ist der Todestag nicht feststellbar, endet die Schutzfrist 110 Jahre nach der Geburt des Betroffenen.

Das Problem im vorliegenden Fall bestand darin, dass diese gesetzlich festgelegten Schutzfristen noch nicht abgelaufen waren. Allerdings können die festgelegten Schutzfristen ausnahmsweise für wissenschaftliche Forschungen verkürzt werden (§ 11 Abs. 5 Saarländisches Archivgesetz). Dies setzt voraus, dass entweder die Betroffenen eingewilligt haben oder die Benutzung für die Durchführung eines bestimmten Forschungsvorhabens erforderlich ist und schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen überwiegt.

Mit dem Ministerium der Justiz war ich der Auffassung, dass eine Verkürzung der Schutzfristen vertretbar und somit eine Einsichtnahme in die fraglichen Personalakten zulässig war.

Nicht einverstanden war ich dagegen mit der beabsichtigen Veröffentlichung von Kurzbiografien dieses Personenkreises. Denn gemäß § 11 Abs. 5 Satz 3 Saarländisches Archivgesetz dürfen personenbezogene Daten in Forschungsergebnissen außer bei Vorliegen einer Einwilligung der Betroffenen nur veröffentlicht werden, wenn dies für die Darstellung von Forschungsergebnissen unerlässlich ist. Im Zusammenhang mit historischer Forschung verstehe ich diese Vorschrift so, dass bei Darstellung von Ereignissen der Zeitgeschichte auch die Nennung der Namen der handelnden Personen zulässig ist. In diesem Fall ist der Personenbezug unerlässlich im Sinne der Vorschrift. Vorliegend sollte die Veröffentlichung der Kurzbiografien allein an die Tatsache anknüpfen, dass ein Anwalt in einem bestimmten Zeitraum im Saarland als Anwalt zugelassen war.

Ich habe dem Ministerium der Justiz mitgeteilt, dass ich keine Bedenken gegen eine Veröffentlichung hätte bei Einholung einer Einwilligung der Ehefrauen oder Kinder der Betroffenen.

Im Ergebnis habe ich dem Ministerium der Justiz empfohlen, das Einvernehmen mit der Verkürzung der Schutzfristen mit der Auflage zu verbinden, dass eine personenbezogene Veröffentlichung von Kurzbiografien nicht erfolgt.

16.7 Weitergabe von Informationen über einen Mandatsträger an die Presse

Mit einem nicht ganz alltäglichen Fall hatte ich mich aufgrund der Eingabe eines Stadtratsmitgliedes zu befassen.

Der Petent ist freiberuflich tätiger Unternehmer. Er forderte von der Stadt den Ersatz seines Verdienstausfalles, den er aufgrund seiner Teilnahme an Stadtratssitzungen erlitten hatte. Ein solcher Anspruch steht Stadtratsmitgliedern nach den Vorschriften des saarländischen Kommunalselbstverwaltungsgesetzes ausdrücklich zu: „Den durch die Teilnahme an Sitzungen des Gemeinderates und seiner Ausschüsse entstandenen Verdienstausfall hat die Gemeinde in der nachgewiesenen Höhe zu ersetzen.“ (§ 51 Abs. 3 Satz 1 KSVG) Dass ein solcher Anspruch dem Grund nach besteht, wurde von dem Bürgermeister der betroffenen Stadt nie bestritten.

Im Rahmen eines Pressetermins hat der Bürgermeister der betreffenden Stadt verschiedene Pressevertreter darüber informiert, dass der Petent für den Zeitraum eines Jahres rund 10.000,-- DM Erstattung seines Verdienstausfalles fordere.

In der örtlichen Presse wurde daraufhin das Verhalten des Petenten mit Äußerungen kommentiert wie: „Es gibt genügend Geschäftsleute, die den Spagat zwischen Berufsleben und ehrenamtlichem Engagement in der Politik ohne den Griff in die öffentliche Kasse schaffen." „Die Bürger werden ihm dieses gierige Verhalten nicht abkaufen."

In meiner datenschutzrechtlichen Bewertung bin ich zu dem Ergebnis gekommen, dass die Weitergabe der Information über den geltend gemachten Verdienstausfall an verschiedene Medien datenschutzrechtlich nicht zulässig war.

Jede Weitergabe personenbezogener Daten durch öffentliche Stellen ist nur zulässig, wenn eine entsprechende Rechtsvorschrift die Datenweitergabe legitimiert oder der Betroffene ausdrücklich eingewilligt hat (§ 4 Abs. 1 Saarländisches Datenschutzgesetz).

Auf die Vorschriften des Saarländischen Pressegesetzes (heute: Saarländisches Mediengesetz) konnte die Informationsweitergabe nicht gestützt werden. Das Informationsrecht der Presse war in § 4 des Saarländischen Pressegesetzes (heute: § 5 Mediengesetz) geregelt. Nach § 4 Abs. 1 Pressegesetz waren die Behörden zwar verpflichtet, den Vertretern der Presse die der Erfüllung ihrer öffentlichen Aufgabe dienenden Auskünfte zu erteilen. Auskünfte konnten allerdings unter anderem verweigert werden, soweit ein überwiegendes öffentliches oder schutzwürdiges privates Interesse verletzt würde (§ 4 Abs. 2 Nr. 3 Pressegesetz). Für mich war schon fraglich, welches anerkennenswerte Interesse die Öffentlichkeit an der Information haben soll, dass ein namentlich benanntes Stadtratsmitglied einen ihm gesetzlich ausdrücklich zustehenden Anspruch geltend macht. Jedenfalls lagen aber überwiegende schutzwürdige private Interessen an einer Nichtveröffentlichung vor, zumal die Höhe der Verdienstausfallforderung Rückschlüsse auf das Einkommen des Betroffenen ermöglichte, welches eindeutig seiner Privatsphäre zuzuordnen ist.

Der Bürgermeister der betreffenden Stadt hatte im Schriftwechsel mit meiner Behörde versucht, die Informationsweitergabe damit zu rechtfertigen, dass der Petent Widerspruch gegen die bewilligte Höhe des geltend gemachten Verdienstausfalles eingelegt habe und dieser Widerspruch in öffentlicher Sitzung vor dem Kreisrechtsausschuss verhandelt wurde.

Diesem Argument habe ich entgegen gehalten, dass der Zweck des Öffentlichkeitsprinzips die Kontrolle staatlicher Machtausübung sowie die Förderung des Vertrauens der Allgemeinheit in die Tätigkeit der Verwaltung ist. Diesem Prinzip wird dadurch Rechnung getragen, dass die Allgemeinheit grundsätzlich die Möglichkeit hat, an den Sitzungen des Kreisrechtsausschusses teilzunehmen. Aus dieser Zweckbestimmung lässt sich allerdings nicht die Befugnis der am Widerspruchsverfahren beteiligten Behörden herleiten, die Identität der Widerspruchsführer und den Gegenstand des Widerspruchsverfahrens in der Öffentlichkeit zu verbreiten. Die beteiligte Behörde ist vielmehr an den Grundsatz der Amtsverschwiegenheit gebunden; sie hat, da sie nicht wie der Kreisrechtsausschuss Herr des Verfahrens ist, keinesfalls die Befugnis, die Öffentlichkeit über dessen Verhandlungsgegenstände in personenbezogener Weise zu informieren.

Ich hoffe, dass der geschilderte Fall vielleicht auch bei anderen Kommunen die Sensibilität erhöht, wenn es um die Weitergabe personenbezogener Informationen an die Medien geht.

16.8 Landesamt für Umweltschutz

Bei einer Datenschutzprüfung des Amtes konnte ich feststellen, dass in den Fachbereichen zahlreiche Dateien mit Personenbezug geführt werden, weil Einzelpersonen betroffen sind, die z.B. Heizöltanks besitzen, Wasserrechte nutzen, Schadstoffe in Abwasser einleiten, Eigentümer von Grundstücken mit die Umwelt beeinträchtigenden Altlasten sind oder weil Ordnungswidrigkeiten zu ahnden sind.

Von besonderem Interesse ist das automatisiert geführte **Altlastenkataster**, in dem Grundstücke erfasst werden, bei denen schädliche Bodenveränderungen bestehen oder ein Verdacht begründet ist (z.B. stillgelegte Abfallbeseitigungs-, Tankstellenanlagen oder Gewerbebetriebe). Meiner Forderung, den Umfang der in das Kataster aufzunehmenden Daten zu regeln, wurde inzwischen durch das Saarländische Bodenschutzgesetz vom 20. März 2002 Rechnung getragen (§ 4 Abs. 2 SBodSchG). In dieses Gesetz wurde auch die Bestimmung des Abfallwirtschaftsgesetzes übernommen, dass die Eigentümer und Nutzungsberechtigten der betroffenen Grundstücke über die Eintragung im Altlastenkataster zu unterrichten sind (§ 4 Abs. 3 SBodSchG). Diese Unterrichtung wurde bisher nicht vorgenommen, weil die Eigentümer weitgehend nicht bekannt sind. Ich halte es für unerlässlich, dass das Landesamt sich die erforderlichen Daten beschafft, um die seit 1997 gesetzlich bestehende Informationspflicht den Betroffenen gegenüber zu erfüllen.

Beim Landesamt für Umweltschutz ist ein **Fernmessdienst** für Abwasserbehandlungsanlagen installiert. Zur Überprüfung, ob die Anlagen funktionsgerecht betrieben und die nach den Regeln der Abwassertechnik erreichbare Reinigungsleistung erzielen, werden bestimmte Parameter automatisiert dem Landesamt übermittelt. An das System sind ca. 25 Anlagenbetreiber auf freiwilliger Basis angeschlossen. Das Landesamt hat zugesichert, dass die Anforderungen des § 32 SDSG – Fernmessen und Fernwirken – beachtet werden und dass insbesondere die Betroffenen über die ferngesteuerten Messungen im Detail informiert sind und in die Teilnahme schriftlich eingewilligt haben.

16.9 Staatliches Konservatoramt

Das Staatliche Konservatoramt, bei dem ich eine Datenschutzprüfung vorgenommen habe, führt eine Datenbank der Kulturdenkmäler. In dieser sind zwar überwiegend Objektdaten gespeichert; die Eigentümer waren zum Zeitpunkt der Prüfung noch nicht erfasst. Viele Baudenkmäler im Privatbesitz (z.B. Bauernhäuser) sind jedoch anhand der Angabe von Ort, Straße und Hausnummer ohne weiteres bestimmten Eigentümern zuzuordnen. Auch Unterlagen über gewährte Landeszuwendungen oder über ausgestellte Bescheinigungen für steuerliche Zwecke enthalten ebenso wie Personalvorgänge personenbezogene Daten.

Ich konnte mich im Wesentlichen darauf beschränken, Verbesserungen bei technisch-organisatorischen Maßnahmen der Datensicherung im IT-Bereich (z.B. Zugriffskontrolle, Internetangebot) und beim Zugang zu den Amtsräumen vorzuschlagen.

16.10 Sachverständigenordnung der Industrie- und Handelskammer

Wie mir die Industrie- und Handelskammer (IHK) nach meiner im vergangenen Berichtszeitraum stattgefundenen Prüfung (18. TB, TZ 15.1) mitgeteilt hat, haben sich mehrere Bundesministerien mit den noch offenen Rechtsfragen zum Sachverständigenwesen befasst, da der saarländischen Sachverständigenordnung laut Auskunft der IHK eine einheitliche Musterordnung zugrunde lag.

Mir wurde die ab 1.1.2002 geltende neue Sachverständigenordnung vorgelegt, in der meinen Bedenken weitgehend Rechnung getragen wurde. So ist insbesondere die ehemalige Regelung zur Nachschau in der Wohnung des Sachverständigen, die mit der Verfassung nicht zu vereinbaren schien, entfallen. Die Anzeigepflichten zu Strafverfahren sind den Bestimmungen der Anordnung über Mitteilungen in Strafsachen (MiStra) angeglichen worden.

Ob meiner Empfehlung, im Verfahren zur Bestellung eines Sachverständigen zunächst nur anonymisierte Gutachten vorlegen zu lassen, gefolgt wurde oder aber eine Einwilligung des Gutachten-Auftraggebers durch den zu bestellenden Sachverständigen eingeholt wird, bedarf allerdings noch einer ausdrücklichen Bestätigung durch die IHK bzw. das aufsichtsführende Wirtschaftsministerium.

16.11 Standortverzeichnisse von Mobilfunkantennen

Sowohl der behördliche Datenschutzbeauftragte einer Gemeinde als auch der Städte- und Gemeindetag haben mich um Stellungnahme zu der Frage gebeten, ob es den Kommunen erlaubt sei, Standortverzeichnisse (Kataster) von Mobilfunkantennen zu erstellen. Im Saarland ist diese Frage schon aufgrund fehlender kommunaler Zuständigkeit zu verneinen.

Ich habe auf die landesrechtliche Situation hingewiesen, nach der das Landesamt für Verbraucher-, Gesundheits- und Arbeitsschutz die Anzeige zum Betrieb einer Mobilfunkantenne entgegen nimmt. Als speichernde Stelle für diese Daten, die ich durchaus als personenbeziehbare Daten ansehe, ist dieses Landesamt bei einer Anfrage von Betroffenen zur Auskunft unter Berücksichtigung schutzwürdiger Interessen der Beteiligten nach dem Umweltinformationsgesetz verpflichtet. Die Personenbeziehbarkeit liegt in der Möglichkeit Straße und Hausnummer ohne verhältnismäßig großen Aufwand der Person des Grundstückseigentümers oder –besitzers zuzuordnen. Insofern besteht im Einzelfall die Verpflichtung zwischen dem Recht auf informationelle Selbstbestimmung und dem Interesse der Allgemeinheit an einem freien Zugang zu Umweltinformationen abzuwägen. Auf diese Verpflichtung war allerdings besonders hinzuweisen, da der Personenbezug zunächst nicht erkannt wurde.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich zur Speicherung und Veröffentlichung der Standortverzeichnisse von Mobilfunkantennen geäußert. Für das Erstellen und Veröffentlichen von Katastern, die alle Standorte ausweisen, fehlt bislang eine Rechtsgrundlage, so dass derzeit solche Standortverzeichnisse nicht zulässig sind (Anlage 22).

17 Anlagen

Anlage 1 Biometrische Merkmale in Personalausweisen und Pässen

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001

Im Entwurf eines Terrorismusbekämpfungsgesetzes ist vorgesehen, die Möglichkeit zu eröffnen, in deutschen Personalausweisen und Pässen neben dem Lichtbild und der Unterschrift weitere biometrische Informationen wie zum Beispiel Fingerabdrücke, Handgeometrie, Gesichtsgeometrie u.a. aufzunehmen. Auch die Verwendung genetischer Daten wird nicht ausgeschlossen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass diese Maßnahme schon allein wegen des technischen und zeitlichen Aufwandes, der mit der Einführung derartiger Dokumente verbunden wäre, keinen kurzfristigen Beitrag zur Lösung der mit dem internationalen Terrorismus derzeit verbundenen Probleme leisten kann, zumal Ausländerinnen und Ausländer, die sich in Deutschland aufhalten, nicht erfasst werden.

Die Nutzung biometrischer Merkmale in Personalausweisen und Pässen sowie die damit verbundenen Folgeprobleme (zum Beispiel Art und Ort der Speicherung von Referenzdaten; Vermeidung von Überschussinformationen) werfen eine Vielzahl schwieriger Fragen auf, die einer ausführlichen Diskussion bedürfen. Die zuständigen Stellen werden hierzu aufgefordert, die Notwendigkeit und die rechtlichen und technischen Einzelheiten einer Realisierung dieser Maßnahmen darzulegen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist bereit, sich unter diesen Voraussetzungen mit der Frage zu befassen, ob und wie es möglich ist, mit Hilfe geeigneter zusätzlicher Merkmale in Identifikationspapieren deren Missbrauch zu verhindern, ohne dabei die Grundsätze des Datenschutzes zu verletzen.

Anlage 2 Biometrische Merkmale in Personalausweisen und Pässen

Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07. - 08. März 2002

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eingehend über Geeignetheit, Erforderlichkeit und Angemessenheit der beabsichtigten Einführung biometrischer Merkmale in Ausweisen und Pässen diskutiert. Sie hat ein Positionspapier des Arbeitskreises Technik, das detaillierte Prüfpunkte für die Erprobungsphase einer solchen Maßnahme nennt, zustimmend zur Kenntnis genommen. Für den Fall, dass das Vorhaben trotz noch bestehender Bedenken realisiert werden sollte, hat sie übereinstimmend folgende Anforderungen formuliert:

1. Fälschliche Zurückweisungen berechtigter Personen durch automatisierte Personenerkennungssysteme sind auch bei ständiger Verbesserung der Technik prinzipiell nicht zu vermeiden. Es dürfen deshalb nur Verfahren in Betracht gezogen werden, bei denen die Fehlerquote zumutbar gering ist. In Fehlerfällen muss dafür Sorge getragen werden, dass eine die Betroffenen nicht diskriminierende rasche Aufklärung erfolgt.

2. Zu berücksichtigen ist, dass bei der Anwendung biometrischer Verfahren Zusatzinformationen anfallen können (z.B. Krankheits-, Unfall-, Beschäftigungsindikatoren). Es muss sichergestellt werden, dass die gespeicherten und verarbeiteten Daten keine Rückschlüsse auf zusätzliche personenbezogene Merkmale erlauben.

3. Systeme, die biometrische Daten aus Ausweisen ohne Kenntnis der Betroffenen verarbeiten (sog. passive Systeme), sind abzulehnen.

4. Der Gesetzgeber hat die Verwendung biometrischer Daten in Ausweisen und Pässen grundsätzlich auf die Feststellung beschränkt, dass die dort gespeicherten Daten mit den Merkmalen der jeweiligen Ausweisinhaber und -inhaberinnen übereinstimmen; dies muss erhalten bleiben. Die Verwendung der biometrischen Merkmale für andere öffentliche Zwecke (außer der gesetzlich zugelassenen Verwendung aus dem Fahndungsbestand) wie auch für privatrechtliche Zwecke (Versicherung, Gesundheitssystem) ist auszuschließen. Deshalb hat der Gesetzgeber zu Recht die Einrichtung zentraler Dateien ausgeschlossen. Diese gesetzgeberische Entscheidung darf nicht durch den Aufbau dezentraler Dateien umgangen werden.

5. Die Entscheidung über das auszuwählende biometrische Erkennungssystem verlangt ein abgestimmtes europäisches Vorgehen.

Anlage 3 Veröffentlichung von Insolvenzinformationen im Internet

Entschließung der Datenschutzbeauftragten des Bundes und der Länder
vom 24. April 2001

Dem Bundestag liegt ein Gesetzentwurf der Bundesregierung zur Änderung der Insolvenzordnung (BT-Drs. 14/5680) vor. Danach sollen gerichtliche Entscheidungen – vor allem in Verbraucherinsolvenzverfahren – künftig auch über das Internet veröffentlicht werden können, um Kosten für Bekanntmachungen in Printmedien zu sparen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Informationen aus Insolvenzverfahren, die in das Internet eingestellt sind, durch die Justiz nicht räumlich begrenzt werden können. Darüber hinaus ist deren Speicherung zeitlich nicht beherrschbar, und die Daten können vielfältig ausgewertet werden. Dies kann dazu führen, dass Dritte, etwa Auskunfteien oder Wirtschaftsinformationsdienste, die Daten auch nach Abschluss eines Insolvenzverfahrens speichern und diese über längere Zeit im Internet verfügbar sind. Die mit der Insolvenzordnung bezweckte Chance der Schuldner auf einen wirtschaftlichen Neubeginn würde letztlich auf Dauer beeinträchtigt, wenn sie zeitlebens weltweit abrufbar am Schulden-Pranger stehen.

Der Gesetzgeber muss das Risiko für die betroffenen Verbraucherinnen und Verbraucher, auf Grund einer möglichen Auswertung justizieller Veröffentlichungen im Internet dauerhaft Einbußen bei der Teilnahme am Wirtschaftsverkehr zu erleiden, sorgfältig mit dem Interesse an der beabsichtigten Senkung von Bekanntmachungskosten abwägen. Hierbei ist auch die gesetzgeberische Wertung zu berücksichtigen, dass Personen, für die ein Insolvenzverfahren eröffnet wurde, gerade nicht in das Schuldnerverzeichnis beim Amtsgericht aufgenommen werden. Das Internet bietet im Gegensatz zu einem gerichtlichen Verzeichnis letztlich keine Gewähr, die ordnungsgemäße Pflege und die Löschung personenbezogener Daten sicherzustellen, die für die Betroffenen von entscheidender wirtschaftlicher Bedeutung sein können. Die Datenschutzbeauftragten appellieren daher an den Gesetzgeber und an die Justizverwaltungen der Länder, die aufgezeigten Risiken insbesondere für Verbraucherinsolvenzen neu zu bewerten. Die vorgenannten Überlegungen sind im Gesetzgebungsverfahren bisher nicht in ausreichendem Maße berücksichtigt worden. Dabei sollten die Erwägungen des Bundesverfassungsgerichts im Beschluss vom 09.03.1988 – 1 BvL 49/86 – zu einem vergleichbaren Sachverhalt einbezogen werden.

Es erscheint zu einfach, die Informationen im Internet in gleicher Weise abzubilden wie in der Zeitung. Gerade das Internet bietet neue Chancen und Möglichkeiten, Informationen gezielt nur denen zugänglich zu machen, die es angeht. Gerade hier sind neue Wege möglich, die mit herkömmlichen Medien nicht erreicht werden konnten. Es gilt deshalb, insbesondere zu untersuchen, ob dem Prinzip der Publizität bei Veröffentlichungen im Internet nicht ein anderer Stellenwert zukommt und wie gravierende Nachteile für die Betroffenen vermieden werden können.

Anlage 4 Anlasslose DNA-Analyse aller Männer verfassungswidrig

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12. März 2001

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist entschieden den Vorschlag zurück, den "genetischen Fingerabdruck" aller Männer zu erheben und rein vorsorglich zu speichern. Die Erhebung personenbezogener Daten ist auch im Rahmen der Strafverfolgung an rechtsstaatliche Grundsätze gebunden. Eine Datenerhebung auf Vorrat, die die Hälfte der Bevölkerung als potentielle Straftäter behandelt, ist verfassungsrechtlich unzulässig. Darüber hinaus erscheint der erwartete Abschreckungseffekt äußerst fragwürdig.

Anlage 5 EUROJUST – Vorläufer einer künftigen europäischen Staatsanwaltschaft?

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001

Der Europäische Rat hat im Herbst 1999 in Tampere die Einrichtung einer gemeinsamen Stelle EUROJUST zur justiziellen Zusammenarbeit beschlossen. EUROJUST soll zur Bekämpfung der schweren organisierten Kriminalität eine sachgerechte Koordinierung der nationalen Staatsanwaltschaften erleichtern und die strafrechtlichen Ermittlungen unterstützen sowie die Erledigung von Rechtshilfeersuchen vereinfachen. Zusätzlich beschloss der Rat im Dezember 2000 die Einrichtung einer vorläufigen Stelle zur justiziellen Zusammenarbeit, PRO-EUROJUST genannt, die am 1. März 2001 ihre Arbeit aufgenommen hat. Diese Stelle soll bis zur Einrichtung von EUROJUST die Zusammenarbeit der Ermittlungsbehörden auf dem Gebiet der Bekämpfung der schweren grenzüberschreitenden Kriminalität verbessern und die Koordinierung von Ermittlungen anregen und verstärken. Ein Beschluss des Rates über die Einrichtung von EUROJUST soll bis Ende des Jahres 2001 verabschiedet werden.

Die Aufgabenstellung von EUROJUST führt möglicherweise dazu, dass eine europäische Großbehörde heranwächst, die Daten nicht nur über verdächtige Personen, sondern auch über Opfer und Zeugen sammeln soll, und damit zwangsläufig tiefgreifende Eingriffe in Bürgerrechte vornehmen würde. In diesem Falle käme als Grundlage für EUROJUST nur eine Konvention in Betracht, da für künftige Grundrechtseingriffe durch EUROJUST eine demokratische Legitimation notwendig wäre.

Mit Blick auf die sensiblen personenbezogenen Daten, die von EUROJUST erhoben, verarbeitet und genutzt werden sollen, und unter Berücksichtigung der eigenen Rechtspersönlichkeit von EUROJUST sind umfassende Datenschutzvorschriften erforderlich. Diese müssen sowohl Regelungen zur Verarbeitung, Speicherung, Nutzung, Berichtigung, Löschung als auch zum Auskunftsanspruch des Betroffenen sowie zu einer Kontrollinstanz von EUROJUST enthalten.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sind folgende datenschutzrechtliche Anforderungen an EUROJUST zu stellen:

- Informationsaustausch mit Partnern
  Der Informationsaustausch mit Partnern sollte EUROJUST dann erlaubt sein, wenn er zur Erfüllung seiner Aufgaben erforderlich ist. Bei Weiterleitung dieser Daten an Drittstaaten und –stellen ist die Zustimmung des Mitgliedstaates einzuholen, von dem diese Daten geliefert wurden. Sind personenbezogene Daten betroffen, so muss grundsätzlich eine Übereinkunft zwischen EUROJUST und der Partnerstelle über den Datenschutzstandard getroffen werden. Nur in absoluten Ausnahmefällen, die einer restriktiven Regelung bedürfen, sollte eine Datenübermittlung auch bei Fehlen einer solchen Vereinbarung zulässig sein.

- Verarbeitung personenbezogener Daten
  Der Katalog der personenbezogenen Daten, die automatisiert verarbeitet werden dürfen, ist streng am Maßstab der Erforderlichkeit und an den Aufgaben von EUROJUST zu orientieren. Eine zusätzliche Öffnungsklausel, die letztlich die Speicherung aller Daten zulassen würde, ist abzulehnen. Eine Verarbeitung der Daten von Opfern und Zeugen darf, wenn überhaupt erforderlich, nur unter einschränkenden Bedingungen vorgenommen werden.

- Ermittlungsindex und Dateien
  Der Ermittlungsindex sollte so ausgestaltet sein, dass es sich um eine reine Vorgangsverwaltung handelt. Sofern zusätzlich Arbeitsdateien geführt werden, sind sie genau zu bezeichnen.

- Auskunftsrecht
  Wenn EUROJUST Daten verarbeitet, die ursprünglich von einem Mitgliedstaat geliefert wurden, handelt es sich im Ergebnis um Daten von EUROJUST. Insofern ist ein eigener Auskunftsanspruch von Betroffenen gegenüber EUROJUST unverzichtbar. Für den Fall, dass im Strafverfolgungsinteresse oder aus sonstigen Gründen des Gemeinwohls von einer Auskunft an den Betroffenen abgesehen werden soll, muss eine Abwägung mit den Interessen des Betroffenen an einer Auskunftserteilung vorangegangen sein.

- Änderung, Berichtigung und Löschung
  Es sollte auch eine Regelung zur Sperrung von Daten ausgenommen werden, die dazu führt, dass Daten unter bestimmten Voraussetzungen nicht gelöscht, sondern lediglich gesperrt werden.

- Speicherungsfristen
  Sofern Daten nach Ablauf bestimmter sonstiger Fristen zu löschen sind, z.B. nach Ablauf der Verjährungsfrist einzelner Mitgliedstaaten, sollte sich die Speicherungsfrist bei EUROJUST nach der Frist des Mitgliedstaates richten, in dem sie am kürzesten ist, um eine mögliche Umgehung nationaler Löschungsfristen zu vermeiden. Die Prüffristen sollten zwei Jahre betragen und auch für Folgeprüfungen nicht länger sein.

- Datensicherheit
  Erforderlich sind konkrete Vorschriften zur Datensicherheit. Um den Text des Beschlusses nicht zu überfrachten, könnte eine Regelung entsprechend Art. 22 der Verordnung EG 45/2001 oder § 9 BDSG vorgesehen werden.

- Gemeinsame Kontrollinstanz
  Die Erforderlichkeit einer gemeinsamen Kontrollinstanz für EUROJUST muss außer Frage stehen. Die Unabhängigkeit dieser gemeinsamen Kontrollinstanz ist bereits durch die personelle Zusammensetzung zu gewährleisten. Sowohl für die EUROJUST-Mitglieder als auch das Kollegium müssen die Entscheidungen der gemeinsamen Kontrollinstanz bindenden Charakter haben.

- Rechtsschutz
  Dem Betroffenen ist ein angemessener Rechtsschutz gegenüber EUROJUST zu gewähren. Es sollte festgelegt werden, welche nationale oder supranationale Gerichtsbarkeit für Klagen auf Auskunft, Löschung, Berichtigung und Schadensersatz zuständig ist.

- Rechtsetzungsbedarf
  Zur Erfüllung seiner Aufgaben muss EUROJUST Auskünfte über strafrechtliche Ermittlungsverfahren einholen. Nach geltendem Recht (§ 474 StPO) können die Ermittlungsbehörden der Bundesrepublik Deutschland derartigen Ersuchen nicht stattgeben.

  Darüber hinaus bedarf der Zugriff des deutschen EUROJUST-Mitglieds auf das Bundeszentralregister und auf das Zentrale Staatsanwaltschaftliche Verfahrensregister einer eindeutigen gesetzlichen Grundlage.

Anlage 6 Sondertreffen der Datenschutzbeauftragten des Bundes und der Länder zur Terrorismusbekämpfung

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 1. Oktober 2001

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen mit Nachdruck den Kampf des demokratischen Rechtsstaats gegen Terrorismus und organisierte Kriminalität. Sie sind heute zu einem Sondertreffen in Bonn zusammengekommen, um die aktuelle Situation nach den Terroranschlägen zu erörtern. Im politischen Raum werden zahlreiche Forderungen und Vorschläge zur Verbesserung der inneren Sicherheit diskutiert, die auch Auswirkungen auf den Datenschutz haben.

Die Datenschutzbeauftragten weisen darauf hin, dass die Sicherheits- und Strafverfolgungsbehörden zur Terrorismusbekämpfung bereits über weitreichende Befugnisse zur Datenverarbeitung verfügen. So ist z.B. die Rasterfahndung zu Strafverfolgungszwecken generell möglich, in den meisten Ländern auch zur Gefahrenabwehr durch die Polizei. Das Bundesamt für die Anerkennung ausländischer Flüchtlinge kann bereits heute Erkenntnisse über terroristische Aktivitäten an den Verfassungsschutz und die Polizei übermitteln. Auch ist eine effektive Zusammenarbeit zwischen Polizei und Verfassungsschutz durch die geltende Rechtslage gewährleistet; Vollzugsdefizite sind kein Datenschutzproblem. Zu pauschalen Forderungen nach Einschränkung des Bürgerrechts auf Datenschutz besteht deshalb kein Anlass. Die Datenschutzbeauftragten betonen, dass Datenschutz nie Täterschutz war und auch in Zukunft nicht sein wird.

Die Datenschutzbeauftragten sind zu einem offenen und konstruktiven Dialog über etwa notwendige Anpassungen an die neue Bedrohungslage bereit. Sie erwarten, dass sie rechtzeitig beteiligt werden. Die Datenschutzbeauftragten warnen vor übereilten Maßnahmen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger einschränken. Sie sprechen sich dafür aus, alle neu beschlossenen Eingriffsbefugnisse zu befristen und tiefgreifende Eingriffsbefugnisse, damit auch die laufende Rasterfahndung, einer ergebnisoffenen Erfolgskontrolle zu unterziehen.

Bei der künftigen Gesetzgebung sind die grundlegenden Rechtsstaatsprinzipien, das Grundrecht der freien Entfaltung der Persönlichkeit, das Verhältnismäßigkeitsprinzip, die Unschuldsvermutung und das Gebot besonderer gesetzlicher Verwendungsregelungen für sensible Daten selbstverständlich zu beachten. Diese verfassungsrechtlichen Garantien prägen den Rechtsstaat, den wir gemeinsam zu verteidigen haben.

Anlage 7 Freiheits- und Persönlichkeitsrechte dürfen bei der Terrorismusbekämpfung nicht verloren gehen

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass zahlreiche Vorschläge in der gegenwärtigen Debatte um notwendige Konsequenzen aus den Terroranschlägen vom 11. September 2001 die erforderliche sachliche und verantwortungsbewusste Abwägung mit den grundgesetzlich geschützten Freiheits- und Persönlichkeitsrechten der Einzelnen vermissen lassen.

Der Entwurf eines Terrorismusbekämpfungsgesetzes und der Antrag der Länder Baden-Württemberg, Bayern und Hessen im Bundesrat zur wirksamen Bekämpfung des internationalen Terrorismus und Extremismus (BR-Drs. 807/01) übertreffen die in der Entschließung der Konferenz vom 1. Oktober 2001 geäußerte Befürchtung, dass übereilt Maßnahmen ergriffen werden sollen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger unangemessen einschränken.

Gegenwärtig wird ohne Rücksicht auf das grundrechtliche Übermaßverbot vorgeschlagen, was technisch möglich erscheint, anstatt zu prüfen, was wirklich geeignet und erforderlich ist. Außerdem müsste der Frage nachgegangen werden, ob es nicht in den Geheimdiensten und in der Strafverfolgung Vollzugsdefizite gibt. Dabei müsste auch untersucht werden, welche Resultate die vielen Gesetzesverschärfungen der letzten Jahre gebracht haben.

Persönlichkeitsrechte haben über ihre grundrechtssichernde Wirkung hinaus - mit den Worten des Bundesverfassungsgerichts - auch Bedeutung als "elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens".

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert daher sehr eindringlich an alle Beteiligten, nicht Persönlichkeitsrechte vorschnell und ohne die gebotene sorgsam abwägende Prüfung über die bereits bestehenden Eingriffsmöglichkeiten hinaus dauerhaft einzuschränken und so den Ausnahmezustand zur Norm zu erheben.

Alle neu erwogenen Maßnahmen müssen sich daran messen lassen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte so überlagern, dass es in unserem Land zu einer langwirkenden Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommt.

Wesentliche im BMI-Entwurf eines Terrorismusbekämpfungsgesetzes enthaltene Eingriffsmöglichkeiten führen zwangsläufig dazu, dass eine Vielzahl völlig unbescholtener Einzelpersonen zentral erfasst oder verdeckt in Datenerhebungen einbezogen werden, ohne dass eine konkrete Verdachts- oder Gefahrenlage verlangt wird. Zugleich werden Auskunftspflichten und Ermittlungskompetenzen in einer Weise ausgedehnt, dass Eingrenzungen verloren gehen, die aus rechtsstaatlichen Gründen unverzichtbar sind.

Der Verfassungsschutz soll künftig zur Erfüllung aller seiner Aufgaben von den Banken die Kontenbewegungen, von den Luftverkehrsunternehmen alle Reisedaten und von den Post - und Telekommunikationsunternehmen alle Informationen darüber erhalten können, wer von wem Post erhalten und wann mit wem telefoniert hat. All dies soll ohne Wissen der Betroffenen erfolgen und bis zu 15 Jahren gespeichert werden.

Die geplante Befugnis des BKA, Vorermittlungen ohne Anfangsverdacht im Sinne der StPO zu ergreifen, führt zu Eingriffen in das Persönlichkeitsrecht, die weit über das verfassungsrechtlich Zulässige hinausreichen und das tradierte System der Strafverfolgung sprengen. Dies verschiebt die bisher klaren Grenzen zwischen BKA und Verfassungsschutz sowie zwischen Gefahrenabwehr und Strafverfolgung. Ohne jeden Anfangsverdacht soll das BKA künftig Daten über nicht näher eingegrenzte Personenkreise erheben dürfen. Dies kann im Prinzip jede Bürgerin und jeden Bürger betreffen, ohne dass sie sich auf die Schutzmechanismen der Strafprozessordnung verlassen können.

Auch die Vorschläge der Länder enthalten unvertretbare Einschränkungen von grundgesetzlich geschützten Rechtspositionen. So soll die Gefahrenschwelle für den verdeckten Einsatz technischer Mittel in Wohnungen übermäßig abgesenkt werden. Telekommunikationsunternehmen und Internetprovider sollen gesetzlich verpflichtet werden, Verbindungsdaten (zum Beispiel über den Besuch einer Website oder einer Newsgroup) länger zu speichern, als diese zu Abrechnungszwecken benötigt werden, um sie Sicherheitsbehörden zur Verfügung zu stellen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, dass neue Eingriffsbefugnisse nicht pauschal ausgerichtet, sondern zielgenau auf konkrete Gefährdungssituationen im terroristischen Bereich zugeschnitten und von vornherein befristet werden. Eine unabhängige Evaluierung nach festgelegten Fristen ist unerlässlich, um Geeignetheit und Erforderlichkeit für die Zukunft sachgerecht beurteilen zu können.

Anlage 8 Novellierung des G 10-Gesetzes

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09. März 2001

Die Datenschutzbeauftragten des Bundes und der Länder sehen mit großer Sorge, dass die Empfehlungen des Rechts- und des Innenausschusses des Bundesrates erhebliche Einschränkungen der Persönlichkeitsrechte der Bürgerinnen und Bürger zur Folge hätten, die über den Gesetzentwurf der Bundesregierung teilweise weit hinausgehen. Die Datenschutzbeauftragten wenden sich insbesondere entschieden dagegen, dass

- die Befugnisse der Nachrichtendienste zur Übermittlung und Verwendung von G 10-Daten an Strafverfolgungsbehörden gegenüber dem Gesetzentwurf noch deutlich erweitert werden sollen, indem Erkenntnisse der Nachrichtendienste u.a. zur Strafverfolgung weit über die Schwerkriminalität hinaus genutzt werden dürften,
- der Verzicht auf die Kennzeichnung von G 10-Daten sogar ohne vorherige Zustimmung der G 10-Kommission zulässig sein und
- die Schwelle dafür, endgültig von der Benachrichtigung Betroffener abzusehen, deutlich herabgesetzt werden soll.

Darüber hinaus kritisieren die Datenschutzbeauftragten des Bundes und der Länder, dass die Bundesregierung mit der Gesetzesnovelle über die Vorgaben des BVerfG hinaus weitere Änderungen im G 10-Bereich erreichen will, die neue grundrechtliche Beschränkungen vorsehen:

- Die Anforderungen an die halbjährlichen Berichte des zuständigen Bundesministers an die PKG müssen so gefasst werden, dass eine wirksame parlamentarische Kontrolle erreicht wird. Dies ist derzeit nicht gewährleistet. Deshalb muss über Anlass, Umfang, Dauer, Ergebnis und Kosten aller Maßnahmen nach dem G 10-Gesetz sowie über die Benachrichtigung der Beteiligten berichtet werden. Die gleichen Anforderungen müssen auch für die Berichte der PKG an den Bundestag gelten.

- Die Neuregelung, nach der auch außerhalb der Staatsschutzdelikte mutmaßliche Einzeltäter und lose Gruppierungen den Maßnahmen nach dem G 10-Gesetz unterliegen sollen, stellt das Trennungsgebot nach Art. 87 Abs. 1 Satz 2 GG weiter infrage. Ermittlungen von der Eingriffsschwelle eines konkreten Anfangsverdachts zu lösen und nach nachrichtendienstlicher Art schon im Vorfeld zur Verdachtsgewinnung durchzuführen, weitet die Gefahr unverhältnismäßig aus, dass auch gegen Unbescholtene strafrechtlich ermittelt wird.

- Alle Neuregelungen wie z.B. zum Parteienverbotsverfahren, zur Verwendung von G 10-Erkenntnissen bei Gefahren für Leib oder Leben einer Person im Ausland und zu Spontanübermittlungen an den BND müssen befristet und einer effizienten Erfolgskontrolle unterzogen worden.

- Bei der internen Datenverarbeitung durch die Nachrichtendienste ist die Zweckbindung so zu formulieren, dass die erhobenen Daten nicht zur Erforschung und Verfolgung anderer als der in § 3 und § 5 G 10-E genannten Straftaten genutzt werden dürfen.

- Die vorgesehenen Ausnahmen von der vom BVerfG geforderten Kennzeichnungspflicht bei der Übermittlung von Daten, die aus G 10-Maßnahmen stammen, begegnen schwerwiegenden datenschutzrechtlichen Bedenken.

- Im Gesetzentwurf fehlt die Regelung, dass eine Weiterübermittlung an andere Stellen und Dritte nicht zulässig ist. Sie darf nur durch die erhebende Stelle erfolgen. Die Weitergabe von G 10-Daten an andere Dienststellen ist bei der übermittelnden Stelle stets zu dokumentieren und zu kennzeichnen.

- Eine dauerhafte Ausnahme von der Benachrichtigungspflicht ist abzulehnen. Sie würde für die Betroffenen zu einem Ausschluss des Rechtsweges führen.

- Dem BND wird nicht mehr nur die "strategische Überwachung" des nichtleitungsgebundenen, sondern künftig des gesamten internationalen Telekommunikationsverkehrs ermöglicht. Dies setzt den Zugriff deutscher Stellen auf Telekommunikationssysteme in fremden Hoheitsbereichen voraus. Dabei muss sichergestellt werden, dass die Anforderungen des Völkerrechts eingehalten werden.

Die Überwachung internationaler Telekommunikationsbeziehungen im Falle einer Gefahr für Leib oder Leben einer Person im Ausland (§ 8 G 10-E) ermöglicht sehr intensive Grundrechtseingriffe in großer Zahl und mit einer hohen Dichte, die höher sein kann als bei "strategischen Überwachung" nach § 5 G 10-E. Dies setzt eine hohe Eingriffsschwelle und enge zeitliche Befristungen voraus, die der Entwurf nicht hinreichend vorsieht.

Anlage 9 Entwurf des Steuervergünstigungsabbaugesetzes lässt sorgfältige Abwägung zwischen Steuergerechtigkeit und informationellem Selbstbestimmungsrecht vermissen

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

Gesetzesgerechte Steuererhebung und grundrechtlicher Persönlichkeitsschutz stehen in einer Wechselbeziehung, die sorgfältiger Abwägung bedarf. Im Gegensatz zu Bereichen wie Sozialleistungen und Rentenversicherungen, wo es gelungen ist, eine Balance zwischen der wirksamen Erfüllung der staatlichen Aufgaben und dem individuellen Persönlichkeitsrecht des Einzelnen, das sich auch in dem Grundrecht auf informationelle Selbstbestimmung manifestiert, zu finden, lässt der Entwurf des Steuervergünstigungsabbaugesetzes diese Abwägung vermissen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die gesetzgebenden Stellen auf, bei den geplanten Maßnahmen zur Sicherung der Steuergerechtigkeit eine datenschutzkonforme Abwägung zwischen diesen Verfassungsprinzipien vorzunehmen und die Datenschutzrechte der Bürger angemessen zu berücksichtigen. Im Einzelnen machen sie auf Folgendes aufmerksam:

- Die Aufhebung des § 30a AO führt zu einem Wegfall des Bankgeheimnisses und damit zu einer deutlichen Störung des Vertrauensverhältnisses zwischen Banken und Kunden. Dass künftig auch verdachtunabhängige Prüfungen in Banken angeordnet werden können, schafft den "gläsernen Bankkunden" und erweckt den Anschein, als sei jeder Steuerpflichtige ein potentieller Steuerverkürzer. Das datenschutzrechtliche Prinzip, dass Daten grundsätzlich bei Betroffenen zu erheben sind (§ 93a AO), wird außer Kraft gesetzt.

- Der Vertrauensverlust in der Bevölkerung wird durch die automatische Meldepflicht verschärft, die die Banken und andere Finanzdienstleister künftig gegenüber dem Bundesamt für Finanzen (BfF) haben.

- Nach § 23a EStG-E haben die Kreditinstitute Kontrollmitteilungen an das BfF über private Veräußerungsgeschäfte, insbesondere bei Wertpapieren, aber auch bei anderen Wirtschaftsgütern, z.B. Antiquitäten, mit Namen, Anschaffungs- und Veräußerungsbeträgen sowie Anzahl zu senden.

- Gemäß § 45d EStG-E sollen die Banken alle Kapitalerträge, bei denen ein Abzug von Steuern vorgesehen ist, mit Namen, Beträgen und Freistellungssummen dem BfF anzeigen.

- Da die umfangreichen Datenübermittlungen unter einem einheitlichen Identifikationsmerkmal (§ 139a AO-E) beim BfF zusammengeführt werden sollen, entsteht die Sorge, dass für alle Staatsbürger ein einheitliches Personenkennzeichen ins Auge gefasst wird. Dies widerspricht dem Urteil des Bundesverfassungsgerichts zur Volkszählung vom 15. Dezember 1983, wonach die Erschließung von Datenverbünden durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal nicht zulässig ist.

- Die Zusammenführung der Daten beim Bundesamt der Finanzen schafft eine bundesweite Datensammlung über alle Differenzgewinne und Kapitalerträge sowie sonstige Veräußerungsgewinne und verstärkt die Entwicklung des BfF zum zentralen Datenpool. Es besteht erfahrungsgemäß die Gefahr, dass auch andere Behörden auf solche riesigen Datenbestände zugreifen wollen.

- Die geplante Ausweitung der Befugnis zu Kontrollmitteilungen durch die Neufassung des § 194 Abs. 3 AO verstößt gegen das verfassungsrechtliche Übermaßverbot. Unabhängig von einer zulässigen Verwertung von Zufallsfunden müssen Kontrollmitteilungen über alle steuerpflichtigen Staatsbürger daran gebunden werden, dass tatsächliche Anhaltspunkte für den Verdacht einer Steuerverkürzung bereits entstanden sind. Die gegenwärtig geplante verdachtunabhängige Befugnis zu Kontrollmitteilungen ist unverhältnismäßig.

  In diesem Zusammenhang müsste es gesetzlich ausgeschlossen werden, dass kopierte Unterlagen der Betriebe i.S. des § 147 Abs. 6 AO in den Finanzämtern für die massenhafte Herstellung von Kontrollmitteilungen verwendet werden. Da die bisherige Einschränkung des § 194 Abs. 3 AO aufgegeben wird, stehen gesetzlich keine Hindernisse gegen eine solche Auswertung der betrieblichen EDV im Wege. Dies wäre ebenfalls ein Verstoß gegen das verfassungsrechtliche Prinzip der Verhältnismäßigkeit.

Die Konferenz der Datenschutzbeauftragten von Bund und Ländern weist in diesem Zusammenhang darauf hin, dass eine Abgeltungssteuer wie in anderen europäischen Staaten (etwa Österreich und Schweiz) zu vergleichbarem Steueraufkommen führen wird, ohne dass die Banken zu umfassenden Anzeigepflichten über alle Steuerpflichtigen gezwungen werden. Die neuen Überlegungen der Bundesregierung gehen offenbar in diese Richtung und würden damit die Voraussetzungen schaffen, dass Kontrollmitteilungen entfielen, das Bankgeheimnis gewahrt bliebe und es bei Betriebsprüfungen weiterhin ausschließlich um die zulässige Verwertung von Zufallskunden ginge.

Anlage 10 Novellierung des Melderechtsrahmengesetzes

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09. März 2001 *

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Absicht der Bundesregierung, das Melderechtsrahmengesetz im Hinblick auf die neuen Informations- und Kommunikationstechnologien zu modernisieren und einzelne unnötige Meldepflichten abzuschaffen.

1. Allerdings sind aus dem vorliegenden Gesetzentwurf Tendenzen zu erkennen, dass durch den Zusammenschluss mehrerer Melderegister übergreifende Dateien entstehen können, die letztlich sogar zu einem zentralen Melderegister führen würden. Eine solche Entwicklung wäre aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil damit das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger unverhältnismäßig eingeschränkt werden würde.

2. Bereits die bisherige Rechtslage, nach der nahezu jedermann eine einfache Melderegisterauskunft von der Meldebehörde erhalten kann, ist äußerst unbefriedigend. Dies wird dadurch verschärft, dass der Gesetzentwurf - wie in seiner Begründung ausdrücklich betont wird – nunmehr vorsieht, einfache Melderegisterauskünfte mit Hilfe des Internet durch jedermann auch elektronisch abrufen zu können. Um sich gegen eine unkontrollierte Weitergabe solcher über das Internet zum Abruf bereitgehaltener Daten schützen zu können und weil beim Internetgestützten Abruf die gesetzlich vorgeschriebene Berücksichtigung der schutzwürdigen Belange Betroffener nicht möglich ist, sollte für die Bürgerin oder den Bürger in diesen Fällen ein ausdrückliches Einwilligungsrecht oder mindestens ein Widerspruchsrecht geschaffen werden. Es handelt sich hier um personenbezogene Daten, die auf der Grundlage einer gesetzlichen Auskunftspflicht erhoben wurden.

3. Auch für öffentliche Stellen sollte in das Gesetz eine Bestimmung aufgenommen werden, wonach bei elektronischen Abrufverfahren über das Internet zur Wahrung der schutzwürdigen Interessen der Betroffenen zumindest Verfahren der fortgeschrittenen elektronischen Signatur gemäß den Regelungen des Signaturgesetzes einzusetzen sind.

4. Nach geltendem Recht ist jede Melderegisterauskunft unzulässig, wenn eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange glaubhaft gemacht wird. Diese Regelung hat sich bewährt. Die Datenschutzbeauftragten treten angesichts des in diesen Fällen bestehenden hohen Schutzbedarfs dem Vorhaben entschieden entgegen, diese Regelung durch eine Risikoabwägung im Einzelfall aufzuweichen.

5. Bislang dürfen Meldebehörden an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen Auskunft über Daten von Gruppen von Wahlberechtigten erteilen, sofern die Wahlberechtigten dieser Auskunftserteilung nicht widersprochen haben. Die Datenschutzbeauftragten bekräftigen ihre bereits in der Vergangenheit erhobene Forderung, gesetzlich zu regeln, dass eine Einwilligung der Betroffenen Voraussetzung für solche Datenweitergaben sein muss. Die bisherige Widerspruchslösung ist in weiten Kreisen der Bevölkerung unbekannt.

6. Außerdem fordern die Datenschutzbeauftragten, die Hotelmeldepflicht abzuschaffen, da die hiermit verbundene millionenfache Datenerhebung auf Vorrat unverhältnismäßig ist.

* Bei Enthaltung Thüringens zu Ziffer 6.

Anlage 11 Datenschutzrechtliche Anforderungen an den "Arzneimittelpass" (Medikamentenchipkarte)

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001

Vor dem Hintergrund der Lipobay-Diskussion hat das Bundesministerium für Gesundheit die Einführung eines "Arzneimittelpasses" in Form einer (elektronisch nutzbaren) Medikamentenchipkarte befürwortet; auf der Karte sollen alle ärztlichen Verordnungen verzeichnet werden. Damit soll eine größere Transparenz der Arzneimittelverordnungen erreicht werden. Bisher ist nicht ansatzweise belegt, dass die bekannt gewordenen Gefahren für die Patientinnen und Patienten dadurch entstanden sind, dass verschiedene Ärztinnen und Ärzte ohne Kenntnis voneinander unverträgliche Medikamente verordnet hätten. Deswegen ist auch nicht ersichtlich, dass die aufgetretenen Probleme mit einem Arzneimittelpass hätten verhindert werden können.

Aus datenschutzrechtlicher Sicht bestehen erhebliche Bedenken gegen eine Medikamentenchipkarte als Pflichtkarte. Die Datenschutzbeauftragten begrüßen es daher ausdrücklich, dass der Gedanke einer Pflichtkarte fallen gelassen wurde. Die Patientinnen und Patienten würden sonst rechtlich oder faktisch gezwungen, die ihnen verordneten Medikamente und damit zumeist auch ihre Erkrankung bei jedem Arzt- und/oder Apothekenbesuch ohne ihren Willen zu offenbaren. Dies würde eine wesentliche Einschränkung des Arztgeheimnisses bewirken, das auch gegenüber anderen Ärztinnen und Ärzten gilt. Zudem würde sich dadurch das Vertrauensverhältnis, das für die Behandlung und für eine funktionierende Gesundheitsfürsorge insgesamt unabdingbar ist, grundlegend verändern. Darüber hinaus wäre das Einholen einer unbeeinflussten Zweitmeinung nahezu ausgeschlossen.

Die freie und unbeeinflusste Entscheidung der Patientinnen und Patienten über Einsatz und Verwendung der Karte muss gewährleistet werden (Grundsatz der Freiwilligkeit).

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits auf ihrer 47. Konferenz im März 1994 und auf ihrer 50. Konferenz im November 1995 zum freiwilligen Einsatz von Chipkarten im Gesundheitswesen Stellung genommen; deren Zulässigkeit wird dort von verschiedenen Bedingungen zur Sicherung des Persönlichkeitsrechts der Patientinnen und Patienten abhängig gemacht. Grundlegende Voraussetzung ist vor allem die freie Entscheidung der Betroffenen (auch als Versicherte). Sie müssen entscheiden können,

- ob ihre Daten auf einer Chipkarte gespeichert werden,
- welche ihrer Gesundheitsdaten auf die Karte aufgenommen werden,
- welche ihrer Daten auf der Karte wieder gelöscht werden,
- ob sie die Karte bei einem Arzt- oder Apothekenbesuch vorlegen und
- welche ihrer Daten sie im Einzelfall zugänglich machen (die Technik muss eine partielle Freigabe ermöglichen).

Die Verantwortung für die Wahrung der Arzneimittelsicherheit tragen grundsätzlich die Ärztinnen und Ärzte sowie die Apothekerinnen und Apotheker. Sie darf nicht auf die Betroffenen abgewälzt werden. Dies gilt auch, wenn sie von dem "Arzneimittelpass" keinen Gebrauch machen.

Der Chipkarteneinsatz darf nicht zur Entstehung neuer zentraler Datensammlungen über Patientinnen und Patienten führen.

Datenschutzrechtlich problematisch wäre es, den "Arzneimittelpass" auf der Krankenversichertenkarte gemäß § 291 SGB V zu implementieren. Eine solche Erweiterung wäre allenfalls vertretbar, wenn die "Funktion Krankenversichertenkarte" von der "Funktion Arzneimittelpass" informationstechnisch getrennt würde, so dass die Patientinnen oder Patienten bei einem Arzt- oder Apothekenbesuch nicht gezwungen werden, ihre gesamten Gesundheitsdaten ungewollt zu offenbaren. Ihre Entscheidungsfreiheit, wem gegenüber sie welche Gesundheitsdaten offenlegen, müsste also durch die technische Ausgestaltung der Karte gewährleistet sein.

Die Betroffenen müssen ferner das Recht und die Möglichkeit haben, ihre auf der Chipkarte gespeicherten Daten vollständig zu lesen.

Die Verwendung der Karte außerhalb des medizinischen Bereichs, z.B. durch Arbeitgeberinnen und Arbeitgeber oder Versicherungen, muss gesetzlich verboten und sanktioniert werden.

Anlage 12 Gesetzliche Regelung von genetischen Untersuchungen

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder konkretisiert ihre Forderungen an Bundestag und Bundesrat, genetische Untersuchungen am Menschen gesetzlich zu regeln. Geboten sind besondere Regelungen für genetische Untersuchungen zu medizinischen Zwecken, zur Klärung von Identität und Abstammung, im Zusammenhang mit Arbeits- und Versicherungsverhältnissen sowie zu Forschungszwecken. Außer dem "genetischen Fingerabdruck" für Zwecke der Strafverfolgung - in der Strafprozessordnung bereits normiert - sind typische Anwendungsfelder für genetische Untersuchungen zu regeln. Von besonderer Bedeutung sind das Informations- und Entscheidungsrecht der betroffenen Personen. Die Kernanliegen der Datenschutzbeauftragten sind:

- Stärkung des Selbstbestimmungsrechts durch einen grundsätzlichen Einwilligungsvorbehalt für die Durchführung genetischer Untersuchungen;
- Information und Transparenz für die betroffene Person durch Umschreibung des notwendigen Aufklärungsumfangs;
- Qualität und Sicherheit genetischer Tests durch Arzt- und Zulassungsvorbehalte;
- Schutz von Ungeborenen, Minderjährigen und nicht einsichtsfähigen Personen durch abgestufte Beschränkung zugelassener Untersuchungsziele;
- Gewährleistung des Rechts auf Nichtwissen durch differenzierte Entscheidungs- und Offenbarungsoptionen;
- Verhinderung heimlicher Gentests durch das Gebot der Probennahme direkt in ärztlicher Praxis oder Labor;
- Verhinderung von missbräuchlicher Nutzung genetischer Erkenntnisse im Arbeitsleben und im Versicherungsverhältnis durch ein grundsätzliches Verbot, Gentests oder Testergebnisse zu fordern oder entgegen zu nehmen;
- Selbstbestimmung der Betroffenen auch im Forschungsbereich durch einen grundsätzlichen Einwilligungsvorbehalt bei einzelnen Forschungsprojekten und Proben- und Gendatenbanken;
- Sicherung zuverlässiger Pseudonymisierungsverfahren bei Proben- und Gendatenbanken durch externe Datentreuhänderschaft;
- Hilfe für die Betroffenen durch die Pflicht, im Rahmen der Forschung, individuell bedeutsame Untersuchungsergebnisse mitzuteilen;
- Absicherung der Regelungen durch die Einführung von Straftatbeständen.

Neben diesen bereichsspezifischen Bestimmungen zu den verschiedenen Zwecken genetischer Untersuchungen fordert die Konferenz der Datenschutzbeauftragten eine grundlegende Strafnorm im Strafgesetzbuch, um Gentests ohne gesetzliche Ermächtigung oder ohne die grundsätzlich nur für Zwecke der medizinischen Behandlung oder Forschung wirksame Einwilligung der betroffenen Person zu unterbinden.

Die Datenschutzbeauftragten des Bundes und der Länder verstehen ihre Vorschläge als Anregungen zu anstehenden Gesetzesinitiativen und zur gesellschaftspolitischen Diskussion.

Anlage 13 Datenschutzgerechte Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz

Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07.03. - 08.03.2002

Immer mehr Beschäftigte erhalten die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten und ihrer Kommunikationspartner bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben der dienstlichen die private Nutzung des Internet am Arbeitsplatz gestattet wird. Der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat detaillierte Hinweise hierzu erarbeitet.

Insbesondere gilt Folgendes:

1. Die Arbeitsplätze mit Internet-Zugang sind so zu gestalten, dass keine oder möglichst wenige personenbezogene Daten erhoben werden. Die Nutzung des Internet am Arbeitsplatz darf nicht zu einer vollständigen Kontrolle der Bediensteten führen. Präventive Maßnahmen gegen eine unbefugte Nutzung sind nachträglichen Kontrollen vorzuziehen.

2. Die Beschäftigten sind umfassend darüber zu informieren, für welche Zwecke sie einen Internet-Zugang am Arbeitsplatz nutzen dürfen und auf welche Weise der Arbeitgeber die Einhaltung der Nutzungsbedingungen kontrolliert.

3. Fragen der Protokollierung und einzelfallbezogenen Überprüfung bei Missbrauchsverdacht sind durch Dienstvereinbarungen zu regeln. Die Kommunikation von schweigepflichtigen Personen und Personalvertretungen muss vor einer Überwachung grundsätzlich geschützt bleiben.

4. Soweit die Protokollierung der Internet-Nutzung aus Gründen des Datenschutzes, der Datensicherheit oder des ordnungsgemäßen Betriebs der Verfahren notwendig ist, dürfen die dabei anfallenden Daten nicht zur Leistungs- und Verhaltenskontrolle verwendet werden.

5. Wird den Beschäftigten die private E-Mail-Nutzung gestattet, so ist diese elektronische Post vom Telekommunikationsgeheimnis geschützt. Der Arbeitgeber darf ihren Inhalt grundsätzlich nicht zur Kenntnis nehmen, und hat dazu die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen.

6. Der Arbeitgeber ist nicht verpflichtet, die private Nutzung des Internet am Arbeitsplatz zu gestatten. Wenn er dies gleichwohl tut, kann er die Gestattung unter Beachtung der hier genannten Grundsätze davon abhängig machen, dass die Beschäftigten einer Protokollierung zur Durchführung einer angemessenen Kontrolle der Netzaktivitäten zustimmen.

7. Die gleichen Bedingungen wie bei der Nutzung des Internet müssen prinzipiell bei der Nutzung von Intranets gelten.

Die Datenschutzbeauftragten fordern den Bundesgesetzgeber auf, auch wegen des Überwachungspotentials moderner Informations- und Kommunikationstechnik am Arbeitsplatz die Verabschiedung eines umfassenden Arbeitnehmerdatenschutzgesetzes nicht länger aufzuschieben.

Anlage 14 Neue Medienordnung

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001

Bund und Länder beraten gegenwärtig über die Grundzüge einer neuen Medienordnung. Zu den dabei zu beachtenden verfassungsrechtlichen Rahmenbedingungen gehören neben den Gesetzgebungskompetenzen von Bund und Ländern auch die Grundrechte auf Schutz der Privatsphäre und der personenbezogenen Daten, Meinungsfreiheit und Vertraulichkeit der Kommunikation. Diese Rechte müssen in einer neuen Medienordnung durchgängig gewährleistet bleiben.

Angesichts der technischen Entwicklung und der Konvergenz der Medien darf der Grad der Vertraulichkeit nicht mehr allein davon abhängig sein, ob ein Kommunikationsvorgang der Telekommunikation, den Tele- oder den Mediendiensten zugeordnet wird. Vielmehr muss für alle Formen der Kommunikation und der Mediennutzung ein angemessen hoher Schutz gewährleistet werden.

Aus diesem Grund fordert die Konferenz, das Fernmeldegeheimnis nach Art. 10 GG zu einem allgemeinen Kommunikations- und Mediennutzungsgeheimnis weiter zu entwickeln und einfachgesetzlich abzusichern.

Die Konferenz tritt in diesem Zusammenhang dafür ein, die einschlägigen Rechtsvorschriften inhaltlich stärker einander anzugleichen, klarer zu strukturieren und für Nutzende und Anbietende verständlicher zu gestalten.

Anlage 15 Datenschutz bei der Bekämpfung von Datennetzkriminalität

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09. März 2001

Der Europarat entwirft gegenwärtig zusammen mit anderen Staaten, insbesondere den USA und Japan, eine Konvention über Datennetzkriminalität (Cyber-crime-Konvention), die über ihren Titel hinaus auch die automatisierte Speicherung von Daten im Zusammenhang mit anderen Straftaten regeln soll.[1]

Die Datenschutzbeauftragten des Bundes und der Länder verkennen nicht, dass das Internet – ebenso wie andere technische Hilfsmittel – für Straftaten missbraucht wird. Sie teilen daher die Auffassung des Europarats, dass der Kriminalität auch im Internet wirksam begegnet werden muss. Allerdings ist zu beachten, dass sich die weit überwiegende Anzahl der Nutzenden an die gesetzlichen Vorgaben hält. Insoweit stellt sich die Frage der Verhältnismäßigkeit von Maßnahmen, die alle Nutzenden betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder teilen die Auffassung der Europäischen Kommission, dass zur Schaffung einer sichereren Informationsgesellschaft in erster Linie die Sicherheit der Informationsinfrastruktur verbessert werden und anonyme wie pseudonyme Nutzungsmöglichkeiten erhalten bleiben müssen; über Fragen der Bekämpfung der Datennetzkriminalität sollte ein offener Diskussionsprozess unter Einbeziehung der Betreiberinnen und Betreiber, Bürgerrechtsorganisationen, Verbraucherverbände und Datenschutzbeauftragten geführt werden. [2]

Die Konferenz regt eine entsprechende Debatte auch auf nationaler Ebene an und bittet die Bundesregierung, hierfür den erforderlichen Rahmen zu schaffen.

Die Konferenz der Datenschutzbeauftragten fordert die Bundesregierung auf, sich bei der Schaffung von nationalen und internationalen Regelungen zur Bekämpfung von Datennetzkriminalität dafür einzusetzen, dass

- Maßnahmen zur Identifikation von Internet-Nutzenden, zur Registrierung des Nutzungsverhaltens und Übermittlung der dabei gewonnenen Daten für Zwecke der Strafverfolgung erst dann erfolgen dürfen, wenn ein konkreter Verdacht besteht,
- der Datenschutz und das Fernmeldegeheimnis gewährleistet und Grundrechtseingriffe auf das unabdingbare Maß begrenzt werden,
- der Zugriff und die Nutzung personenbezogener Daten einer strikten und eindeutigen Zweckbindung unterworfen werden,
- Daten von Internet-Nutzenden nur in Länder übermittelt werden dürfen, in denen ein angemessenes Niveau des Datenschutzes, des Fernmeldegeheimnisses und der Informationsfreiheit gewährleistet ist sowie verfahrensmäßige Garantien bei entsprechenden Eingriffen bestehen.

[1] European Committee on Crimes Problems (CDPC), Committee of Experts on Crime in Cyber-Space (PC-CY), Draft Convention on Cyber-crime (PC-CY (2000) Draft No. 25)

[2] Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 26.01.2001 – KOM (2000) 890 endgültig

Anlage 16 Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikationsdiensten

Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07.03. - 08.03.2002

Mit der rasch wachsenden Nutzung des Internet kommt dem datenschutzgerechten Umgang mit den dabei anfallenden Daten der Nutzerinnen und Nutzer immer größere Bedeutung zu. Die Datenschutzbeauftragten haben bereits in der Vergangenheit (Entschließung der 59. Konferenz "Für eine freie Telekommunikation in einer freien Gesellschaft") darauf hingewiesen, dass das Telekommunikationsgeheimnis eine unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft ist. Seine Geltung erstreckt sich auch auf Multimedia- und E-Mail-Dienste.

Die Datenschutzbeauftragten betonen, dass das von ihnen geforderte in sich schlüssige System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt, nach wie vor fehlt. Die Strafprozessordnung (und seit dem 1.1.2002 das Recht der Nachrichtendienste) enthält ausreichende Befugnisse, um den Strafverfolgungsbehörden (und den Nachrichtendiensten) im Einzelfall den Zugriff auf bei den Anbietern vorhandene personenbezogene Daten zu ermöglichen. Für eine zusätzliche Erweiterung dieser Regelungen z.B. hin zu einer Pflicht zur Vorratsdatenspeicherung besteht nicht nur kein Bedarf, sondern eine solche Pflicht würde dem Grundrecht auf unbeobachtete Kommunikation nicht gerecht, weil damit jede Handlung (jeder Mausklick) im Netz staatlicher Beobachtung unterworfen würde.

In keinem Fall sind Anbieter von Tele-, Medien- und Telekommunikationsdiensten berechtigt oder verpflichtet, generell Daten über ihre Nutzerinnen und Nutzer auf Vorrat zu erheben, zu speichern oder herauszugeben, die sie zu keinem Zeitpunkt für eigene Zwecke (Herstellung der Verbindung, Abrechnung) benötigen. Sie können nur im Einzelfall berechtigt sein oder verpflichtet werden, bei Vorliegen ausdrücklicher gesetzlicher Voraussetzungen Nachrichteninhalte, Verbindungsdaten und bestimmte Daten (Nutzungsdaten), die sie ursprünglich für eigene Zwecke benötigt haben und nach den Bestimmungen des Multimedia-Datenschutzrechts löschen müssten, den Strafverfolgungsbehörden (oder Nachrichtendiensten) zu übermitteln.

Anlage 17 Geplanter Identifikationszwang in der Telekommunikation

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Mai 2002

Das Bundesministerium für Wirtschaft und Technologie hat einen Entwurf zur Änderung des Telekommunikationsgesetzes veröffentlicht. Der Entwurf hat das Ziel, jeden Anbieter, der geschäftsmäßig Telekommunikationsdienste erbringt, dazu zu verpflichten, Namen, Anschriften, Geburtsdaten und Rufnummern seiner Kundinnen und Kunden zu erheben. Die Kundinnen und Kunden werden verpflichtet, dafür ihren Personalausweis vorzulegen, dessen Nummer ebenfalls gespeichert werden soll. Die beabsichtigten Änderungen sollen in erster Linie dazu führen, auch Nutzerinnen und Nutzer von Prepaid-Karten (also die Erwerberinnen und Erwerber von SIM-Karten ohne Vertrag) im Mobilfunk erfassen zu können. Die erhobenen Daten sollen allein dem Zweck dienen, den Sicherheitsbehörden zum jederzeitigen Online-Abruf über die Regulierungsbehörde für Telekommunikation und Post bereitzustehen. Im gleichen Zuge sollen die Zugriffsmöglichkeiten der Sicherheitsbehörden auf diese Daten dadurch erheblich erweitert werden, indem auf die Kundendateien nach abstrakten Merkmalen zugegriffen werden kann.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen dieses Vorhaben ab. Unter der unscheinbaren Überschrift "Schließen von Regelungslücken" stehen grundlegende Prinzipien des Datenschutzes zur Disposition. Kritikwürdig an dem geplanten Gesetz sind insbesondere die folgenden Punkte:

- Der geplante Grundrechtseingriff ist nicht erforderlich, um die Ermittlungstätigkeit der Sicherheitsbehörden zu erleichtern. Seine Eignung ist zweifelhaft: Auch die Gesetzesänderung wird nicht verhindern, dass Straftäterinnen und Straftäter bewusst und gezielt in kurzen Zeitabständen neue Prepaid-Karten erwerben, Strohleute zum Erwerb einsetzen, die Karten häufig – teilweise nach jedem Telefonat – wechseln oder die Karten untereinander tauschen. In der Begründung wird nicht plausibel dargelegt, dass mit dem geltenden Recht die Ermittlungstätigkeit tatsächlich behindert und durch die geplante Änderung erleichtert wird. Derzeit laufende Forschungsvorhaben beziehen diese Frage nicht mit ein.

- Der Entwurf widerspricht auch dem in den Datenschutzrichtlinien der Europäischen Union verankerten Grundsatz, dass Unternehmen nur solche personenbezogenen Daten verarbeiten dürfen, die sie selbst zur Erbringung einer bestimmten Dienstleistung benötigen.

- Die Anbieter würden eine Reihe von Daten auf Vorrat speichern müssen, die sie selbst für den Vertrag mit ihren Kunden nicht benötigen. Die ganz überwiegende Zahl der Nutzerinnen und Nutzer von Prepaid-Karten, darunter eine große Zahl Minderjähriger, würde registriert, obwohl sie sich völlig rechtmäßig verhalten und ihre Daten demzufolge für die Ermittlungstätigkeit der Strafverfolgungsbehörden nicht benötigt werden. Das Anhäufen von sinn- und nutzlosen Datenhalden wäre die Folge.

- Die gesetzliche Verpflichtung, sich an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten, würde konterkariert. Gerade die Prepaid-Karten sind ein gutes praktisches Beispiel für den Einsatz datenschutzfreundlicher Technologien, da sie anonymes Kommunizieren auf unkomplizierte Weise ermöglichen. Die Nutzung dieser Angebote darf deshalb nicht von der Speicherung von Bestandsdaten abhängig gemacht werden.

- Mit der Verpflichtung, den Personalausweis vorzulegen, würden die Anbieter zusätzliche Informationen über die Nutzerinnen und Nutzer erhalten, die sie nicht benötigen, z. B. die Nationalität, Größe oder Augenfarbe. Die vorgesehene Pflicht, auch die Personalausweisnummern zu registrieren, darf auch künftig keinesfalls dazu führen, dass die Ausweisnummern den Sicherheitsbehörden direkt zum Abruf bereitgestellt werden und sie damit diese Daten auch für die Verknüpfung mit anderen Datenbeständen verwenden können.

- Auch Krankenhäuser, Hotels, Schulen und Hochschulen sowie Unternehmen und Behörden, die ihren Mitarbeiterinnen und Mitarbeitern das private Telefonieren gestatten, sollen verpflichtet werden, die Personalausweisnummern der Nutzerinnen und Nutzer zu registrieren.

- Die Befugnis, Kundendateien mit unvollständigen oder ähnlichen Suchbegriffen abzufragen, würde den Sicherheitsbehörden eine Vielzahl personenbezogener Daten unbeteiligter Dritter zugänglich machen, ohne dass diese Daten für ihre Aufgaben erforderlich sind. Die notwendige strikte Beschränkung dieser weitreichenden Abfragebefugnis durch Rechtsverordnung setzt voraus, dass ein entsprechender Verordnungsentwurf bei der Beratung des Gesetzes vorliegt.

Der Formulierungsvorschlag des Bundeswirtschaftsministeriums lässt eine Auseinandersetzung mit dem Recht auf informationelle Selbstbestimmung der Kundinnen und Kunden der Telekommunikationsunternehmen weitgehend vermissen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Gesetzgeber auf, auf die geplante Änderung des Telekommunikationsgesetzes zu verzichten und vor weiteren Änderungen die bestehenden Befugnisse der Sicherheitsbehörden durch unabhängige Stellen evaluieren zu lassen.

Anlage 18 Systematische verdachtslose Datenspeicherung in der Telekommunikation und im Internet

Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 24. und 25.10.2002

Gegenwärtig werden sowohl auf nationaler als auch auf europäischer Ebene Vorschläge erörtert, die den Datenschutz im Bereich der Telekommunikation und der Internetnutzung und insbesondere den Schutz des Telekommunikationsgeheimnisses grundlegend in Frage stellen.

Geplant ist, alle Anbieter von Telekommunikations- und Multimediadiensten zur verdachtslosen Speicherung sämtlicher Bestands-, Verbindungs-, Nutzungs- und Abrechnungsdaten auf Vorrat für Mindestfristen von einem Jahr und mehr zu verpflichten, auch wenn sie für die Geschäftszwecke der Anbieter nicht (mehr) notwendig sind. Das so entstehende umfassende Datenreservoir soll dem Zugriff der Strafverfolgungsbehörden, der Polizei und des Verfassungsschutzes bei möglichen Anlässen in der Zukunft unterliegen. Auch auf europäischer Ebene werden im Rahmen der Zusammenarbeit der Mitgliedsstaaten in den Bereichen "Justiz und Inneres" entsprechende Maßnahmen - allerdings unter weitgehendem Ausschluss der Öffentlichkeit - diskutiert.

Die Datenschutzbeauftragten des Bundes und der Länder treten diesen Überlegungen mit Entschiedenheit entgegen. Sie haben schon mehrfach die Bedeutung des Telekommunikationsgeheimnisses als unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft hervorgehoben. Immer mehr menschliche Lebensäußerungen finden heute in elektronischen Netzen statt. Sie würden bei einer Verwirklichung der genannten Pläne einem ungleich höheren Überwachungsdruck ausgesetzt als vergleichbare Lebensäußerungen in der realen Welt. Bisher muss niemand bei der Aufgabe eines einfachen Briefes im Postamt seinen Personalausweis vorlegen oder in einer öffentlichen Bibliothek registrieren lassen, welche Seite er in welchem Buch aufschlägt. Eine vergleichbar umfassende Kontrolle entsprechender Online-Aktivitäten (E-Mail-Versand, Nutzung des WorldWideWeb), wie sie jetzt erwogen wird, ist ebenso wenig hinnehmbar.

Zudem hat der Gesetzgeber erst vor kurzem die Befugnisse der Strafverfolgungsbehörden erneut deutlich erweitert. Die praktischen Erfahrungen mit diesen Regelungen sind von unabhängiger Seite zu evaluieren, bevor weitergehende Befugnisse diskutiert werden.

Die Konferenz der europäischen Datenschutzbeauftragten hat in ihrer Erklärung vom 11. September 2002 betont, dass eine flächendeckende anlassunabhängige Speicherung sämtlicher Daten, die bei der zunehmenden Nutzung von öffentlichen Kommunikationsnetzen entstehen, unverhältnismäßig und mit dem Menschenrecht auf Achtung des Privatlebens unvereinbar wäre. Auch in den Vereinigten Staaten sind vergleichbare Maßnahmen nicht vorgesehen.

Mit dem deutschen Verfassungsrecht ist eine verdachtslose routinemäßige Speicherung sämtlicher bei der Nutzung von Kommunikationsnetzen anfallender Daten auf Vorrat nicht zu vereinbaren. Auch die Rechtsprechung des Europäischen Gerichtshofs lässt eine solche Vorratsspeicherung aus Gründen bloßer Nützlichkeit nicht zu.

Die Konferenz fordert die Bundesregierung deshalb auf, für mehr Transparenz der Beratungen auf europäischer Regierungsebene einzutreten und insbesondere einer Regelung zur flächendeckenden Vorratsdatenspeicherung nicht zuzustimmen.

Anlage 19 Datenschutzgerechte Vergütung für digitale Privatkopien im neuen Urheberrecht

Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 24. und 25.10.2002

Zur Umsetzung der EU-Urheberrechtsrichtlinie wird gegenwärtig über den Entwurf der Bundesregierung für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft beraten. Hierzu hat der Bundesrat die Forderung erhoben, das bisherige System der Pauschalabgaben auf Geräte und Kopiermedien, die von den Verwertungsgesellschaften auf die Urheberinnen und Urheber zur Abgeltung ihrer Vergütungsansprüche verteilt werden, durch eine vorrangige individuelle Lizenzierung zu ersetzen. Zugleich hat der Bundesrat die Gewährleistung eines ausreichenden Schutzes der Nutzerinnen und Nutzer vor Ausspähung personenbezogener Daten über die individuelle Nutzung von Werken und die Erstellung von Nutzungsprofilen gefordert.

Die Datenschutzbeauftragten des Bundes und der Länder weisen in diesem Zusammenhang auf Folgendes hin: Das gegenwärtig praktizierte Verfahren der Pauschalvergütung beruht darauf, dass der Bundesgerichtshof eine individuelle Überprüfung des Einsatzes von analogen Kopiertechniken durch Privatpersonen zur Durchsetzung von urheberrechtlichen Vergütungsansprüchen als unvereinbar mit dem verfassungsrechtlichen Schutz der persönlichen Freiheitsrechte der Nutzerinnen und Nutzer bezeichnet hat. Diese Feststellung behält auch unter den Bedingungen der Digitaltechnik und des Internets ihre Berechtigung. Die Datenschutzkonferenz bestärkt den Gesetzgeber, an diesem bewährten, datenschutzfreundlichen Verfahren festzuhalten. Sollte der Gesetzgeber – wie es der Bundesrat fordert – jetzt für digitale Privatkopien vom Grundsatz der Pauschalvergütung (Geräteabgabe) tatsächlich abgehen wollen, so kann er den verfassungsrechtlichen Vorgaben nur entsprechen, wenn er sicherstellt, dass die urheberrechtliche Vergütung aufgrund von statistischen oder anonymisierten Angaben über die Nutzung einzelner Werke erhoben wird. Auch technische Systeme zur digitalen Verwaltung digitaler Rechte (Digital Rights Management) müssen datenschutzfreundlich gestaltet werden.

Anlage 20 Elektronisches Fahrgeldmanagement (EFM) Datenschutzrechtliche Grundanforderungen

64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 24. und 25.10.2002

1. Transparenz

Die Datenverarbeitung durch das EFM muss transparent sein (§ 6 c Abs. 1 Nr.2 und 3 BDSG). Dies erfordert die

- Festlegung der Zwecke,
- Beschreibung der einzelnen Datenverarbeitungsvorgänge differenziert nach den jeweiligen für den Fahrgast zutreffenden Geschäftsprozessen und die dabei zu verarbeitenden Daten,
- Angaben der Identitäten und Anschriften der Stellen, die zu den genannten Zwecken personenbezogene Daten verarbeiten und/oder bei denen die jeweiligen Rechtsansprüche geltend gemacht und Verfahrensbeschreibungen gem. § 4g Abs. 2 Satz 2 BDSG eingesehen werden können.
- Einbeziehung der Unterrichtungspflichten der Kundenvertragspartner. Dazu sollte ein Merk- oder Informationsblatt erstellt werden, in dem der Fahrgast in allgemein verständlicher Form über die vorgesehene Datenverarbeitung - auch durch zentrale Servicestellen oder andere autorisierte Dritte - und über seine Rechte nach §§ 34,35 BDSG unterrichtet wird.

2. Widerspruchsrecht

Der Verband der Deutschen Verkehrsunternehmen sollte mit seinen Kundenvertragspartnern verabreden, dass der Kunde bei Vertragsabschluss schriftlich erklärt, ob er der Übermittlung oder Nutzung seiner Daten zu Zwecken der Werbung und der Markt- und Meinungsforschung widersprechen möchte oder nicht. Es ist sicherzustellen, dass auch autorisierte Dritte diese Beschränkung beachten.

3. Wahlmöglichkeit

Den Fahrgästen muss nach Information über die vertraglich bedingte Datenverarbeitung eine freie Entscheidung zwischen anonymer Fahrt und besonderen Leistungsangeboten (bspw. best pricing) überlassen bleiben.

4. Datensparsamkeit

Alle Leistungsmerkmale und Geschäftsprozesse sind nach dem Prinzip der Datenvermeidung und Datensparsamkeit (§ 3 a Bundesdatenschutzgesetz) zu gestalten. Insbesondere ist auszuschließen, dass kundenbezogene Bewegungsprofile erstellt werden. Das bedeutet:

- Daten für Planungszwecke und zur Optimierung des Angebots sind anonym zu erheben oder zu anonymisieren;

- soweit Daten für besondere Leistungsangebote oder das Reklamationsmanagement benötigt werden, sind diese pseudonym zu erheben und zu speichern, so dass ohne Wissen und Wollen des betroffenen Fahrgastes eine Zuordnung zu seiner Person ausgeschlossen ist;

- werden zu Zwecken des Reklamationsmanagements nutzungsbezogene Daten auf mobile Speichermedien (Chipkarte) geschrieben, muss es dem Fahrgast ermöglicht werden, diese Daten auf eigene Verantwortung zu löschen.

5. Getrennte Verarbeitung

Es müssen die jeweils erforderlichen technischen und organisatorischen Maßnahmen getroffen werden, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Nr.8 der Anlage zu § 9 BDSG).

6. Zweckbindung der Ticketdaten

Darüber hinaus dürfen keine kunden- oder kartenbezogenen Auswertungen zu fremden Zwecken erfolgen. Zu Abrechnungszwecken im Verkehrsverbund dürfen allenfalls (pseudonyme) kartenbezogene Daten übermittelt werden.

7. Vorabkontrolle

Von dem oder der betrieblichen Datenschutzbeauftragten ist vor Inbetriebnahme des EFM eine Vorabkontrolle durchzuführen (§ 4 d Abs. 5 und 6 BDSG) und zu dokumentieren.

8. Zugriffsberechtigung

Der Lesezugriff für Kontrollpersonal muss auf die zur Kontrolle notwendigen Daten beschränkt sein, insbesondere auf dem Speichermedium des Fahrgastes.

9. Datenschutzgerechte Gestaltung der Systemkomponenten

Die Systemkomponenten, die von Fahrgästen bedient werden, sind datenschutzgerecht so zu gestalten, dass

- keine Möglichkeit für Unbefugte besteht, an Terminals für bargeldlose Zahlung die Eingabedaten, insbesondere Authentifikationsdaten zur Kenntnis zu nehmen,

- Fehlermeldungen der Zugangs-Erfassungssysteme die Betroffenen nicht öffentlich diskriminieren,

- die Fahrgäste in angemessenem Umfang die Möglichkeit haben, den Inhalt der Chipkarte jederzeit auslesen zu können.

10. Schutz gegen Missbrauch

Es müssen Vorkehrungen (beispielsweise Sperrung, Verschlüsselung) getroffen werden, die den Fahrgast in angemessener Weise gegen missbräuchliche Verwendung der Daten durch Dritte bei Verlust des Speichermediums schützen.

11. Löschung

Die Dauer der für die bestimmten Geschäftsprozesse erfolgenden Speicherung personenbezogener Daten muss so kurz wie möglich sein. Für die jeweiligen Geschäftsprozesse sind Regelfristen für die Löschung der Daten festzulegen (§ 4e Satz 1 Nr. 7 BDSG). In den Terminals gespeicherte Daten sind nach erfolgreicher Datenübertragung an den Rechner des Kundenvertragspartners zu löschen.

Anlage 21 Neues Abrufverfahren bei den Kreditinstituten

Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07.03. - 08.03.2002

Nach der Novelle des Gesetzes über das Kreditwesen soll die zuständige Bundesanstalt die von den Kreditinstituten vorzuhaltenden Daten, wer welche Konten und Depots hat, ohne Kenntnis der Kundinnen und Kunden zur eigenen Aufgabenerfüllung oder zu Gunsten anderer öffentlicher Stellen abrufen können. Dies ist ein neuer Eingriff in die Vertraulichkeit der Bankbeziehungen.

Dieser Eingriff in die Vertraulichkeit der Bankbeziehungen muss gegenüber den Kundinnen und Kunden zumindest durch eine aussagekräftige Information transparent gemacht werden. Die Konferenz fordert daher, dass zugleich mit der Einführung dieses Abrufverfahrens eine Verpflichtung der Kreditinstitute zur generellen Information der Kundinnen und Kunden vorgesehen wird und diese die Kenntnisnahme schriftlich bestätigen. Dadurch soll zugleich eine effektive Wahrnehmung des Auskunftsrechts der Kundinnen und Kunden gewährleistet werden.

Die Erweiterung der Pflichten der Kreditinstitute, Kontenbewegungen auf die Einhaltung gesetzlicher Bestimmungen mit Hilfe von EDV-Programmen zu überprüfen, verpflichtet die Kreditinstitute außerdem zu einer entsprechend intensiven Kontenüberwachung (sog. "know your customer principle"). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass die Überprüfung in einer Weise stattfindet, die ein datenschutzkonformes Vorgehen sicherstellt.

Anlage 22 Speicherung und Veröffentlichung der Standortverzeichnisse von Mobilfunkantennen

Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 24. und 25.10.2002

Die Speicherung und die Veröffentlichung der Standortdaten von Mobilfunkantennen durch die Kommunen oder andere öffentliche Stellen stehen zur Zeit in verstärktem Maße in der öffentlichen Diskussion. Mehrere kommunale Spitzenverbände haben sich diesbezüglich bereits an die jeweiligen Landesdatenschutzbeauftragten gewandt. Unbeschadet bereits bestehender Landesregelungen und der Möglichkeit, Daten ohne Grundstücksbezug zu veröffentlichen, fordert die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder aufgrund der bundesweiten Bedeutung der Frage den Bundesgesetzgeber auf, im Rahmen einer immissionsschutzrechtlichen Regelung über die Erstellung von Mobilfunkkatastern zu entscheiden.

Dabei ist zu bestimmen, wie derartige Kataster erstellt werden sollen. Die gegenwärtige Regelung des Bundesimmissionsschutzgesetzes sieht keine ausdrückliche Ermächtigung zur Schaffung von Mobilfunkkatastern vor, so dass deren Erstellung und Veröffentlichung ohne Einwilligung der Grundstückseigentümer und -eigentümerinnen und der Antennenbetreiber keine ausdrückliche gesetzliche Grundlage hat. Bei der Novellierung ist insbesondere zu regeln, ob und unter welchen Bedingungen eine Veröffentlichung derartiger Kataster im Internet oder in vergleichbaren Medien zulässig ist. Individuelle Auskunftsansprüche nach dem Umweltinformationsgesetz oder den Informationsfreiheitsgesetzen bleiben davon unberührt.

Sachverzeichnis

Abkürzungsverzeichnis

ACL	Access Control List
ADV	Automatisierte Datenverarbeitung
ALB	Automatisiertes Liegenschaftsbuch
ALIKA	Automatisiertes Liegenschaftskataster
AO	Abgabenordnung
Artikel 10 G	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
AsylVerfG	Asylverfahrensgesetz
AZRG	Ausländerzentralregistergesetz
BAföG	Bundesausbildungsförderungsgesetz
BDSG	Bundesdatenschutzgesetz
BfV	Bundesamt für Verfassungsschutz
BGS	Bundesgrenzschutz
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BNDG	Gesetz über den Bundesnachrichtendienst
BSI	Bundesamt für die Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidung des Bundesverfassungsgerichts
BZRG	Bundeszentralregistergesetz
DNA	Desoxyribonukleinsäure-Analyse (Molekular genetische Untersuchung)
DV	Datenverarbeitung
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
eGovernment	Elektronic Government
eMail	Elektronisch versandte Post
EU	Europäische Union
GG	Grundgesetz
GGO	Gemeinsame Geschäftsordnung für die Obersten Landesbehörden
GMBl	Gemeinsames Ministerialblatt des Saarlandes
IHK	Industrie- und Handelskammer
IEEE	Institute of Electrical and Electronics Engineers Inc.
INPOL	Verbunddatei der Polizei
INTEL	Fa. Intel-Corp.
IP	Internet Protocol
IPSEC	Internet Protocol Security
IT	Informationstechnik
JGG	Jugendgerichtsgesetz
KSVG	Kommunalselbstverwaltungsgesetz

LDAP	Lightweight Directory Access Protocol – ein Internet-basiertes Zugangsprotokoll für Verzeichnisdienste
LfD	Landesbeauftragter für Datenschutz
LfV	Landesamt für Verfassungsschutz
LKA	Landeskriminalamt
LPM	Landesinstitut für Pädagogik und Medien
LVA	Landesversicherungsanstalt
MAC-Adresse	Media-Access-Control-Adresse
MADG	Gesetz über den Militärischen Abschirmdienst
MiStra	Anordnung über Mitteilungen in Strafsachen
NAT	Network Adress Translation
NJW	Neue Juristische Wochenschrift
PGP	Pretty good privacy: International bekanntes Verschlüsselungsverfahren, das mit öffentlichen und privaten Schlüsseln arbeitet
PIN	Persönliche Geheimnummer
SDSG	Saarländisches Datenschutzgesetz
SGB	Sozialgesetzbuch
SINA	Sichere Inter-Netzwerk Architektur des BSI
Sphinx	Deutsches Pilotprojekt zur Erprobung von Verfahren zur digitalen Signatur und Verschlüsselung
SPolG	Saarländisches Polizeigesetz
SSL	Secure Socket Layer: durch Verschlüsselung gesichertes Übertragungsverfahren im Internet
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
SÜG	Sicherheitsüberprüfungsgesetz
SVerf	Saarländische Verfassung
TB	Tätigkeitsbericht
TESTA	Trans-European Services for Telematics between Administrations – europaweites Netz der öffentlichen Verwaltungen
TK	Telekommunikation
TZ	Textziffer
VO	Verordnung
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wireless-LAN	Lokale Vernetzung auf Funknetzbasis