

**Der Landesbeauftragte für den Datenschutz
Mecklenburg-Vorpommern**



**Fünfter
Tätigkeitsbericht
2000/2001**

Herausgeber:



Der Landesbeauftragte für den Datenschutz
Mecklenburg-Vorpommern
Schloss Schwerin

19053 Schwerin

Telefon: (03 85) 5 94 94-0

Telefax: (03 85) 5 94 94-58

E-Mail: datenschutz@mvnet.de

Internet: <http://www.lfd.m-v.de>

cw Obotritendruck GmbH

Druck:

Vorwort

Das Datenschutzgesetz von Mecklenburg-Vorpommern sieht vor, dass der Landesbeauftragte für den Datenschutz dem Landtag und der Landesregierung für jeweils zwei Kalenderjahre einen Tätigkeitsbericht vorlegt. Der vorliegende Fünfte Tätigkeitsbericht umfasst den Zeitraum vom 1. Januar 2000 bis 31. Dezember 2001.

Wie in den vorherigen Berichten habe ich Vorgänge ausgewählt, die einen Gesamteindruck von der Tätigkeit meiner Behörde vermitteln. Einige Beiträge schließen an Sachverhalte aus den letzten Tätigkeitsberichten an. Insofern könnte es nützlich sein, in dem einen oder anderen Fall noch einmal auf diese Berichte zurückzugreifen.

Für die konstruktive und angenehme Zusammenarbeit danke ich meinen Amtskolleginnen und -kollegen beim Bund und in den Ländern. Ein weiterer Dank gilt meinen Mitarbeiterinnen und Mitarbeitern für die engagierte, zuverlässige und sachkundige Arbeit im Berichtszeitraum sowie bei der Erarbeitung der einzelnen Beiträge dieses Berichtes.

Dr. Werner Kessel

Landesbeauftragter für den Datenschutz
Mecklenburg-Vorpommern

INHALTSVERZEICHNIS

1	EINLEITUNG	11
2	SITUATION DES DATENSCHUTZES	15
3	SORGEN DER BÜRGER, EINZELFÄLLE, BERATUNGEN, KONTROLLEN, STELLUNGNAHMEN, GESETZE, VERORDNUNGEN	21
3.1	RECHTSWESEN	22
3.1.1	Strafverfahrensänderungsgesetz	22
3.1.2	Nachfolgeregelung zu § 12 FAG	22
3.1.3	Parlamentarische Kontrolle von Lauschangriffen	24
3.1.4	Veröffentlichungen der Justiz im Internet	25
3.1.5	Novelliertes G 10-Gesetz.....	27
3.2	NEUES DATENSCHUTZRECHT	29
3.2.1	Die Novellierung des Landesdatenschutzgesetzes (DSG M-V)	29
3.2.2	Novelliertes Bundesdatenschutzgesetz	29
3.2.3	EG-Datenschutzverordnung.....	30
3.2.4	EU-Grundrechte-Charta	32
3.3	POLIZEI	33
3.3.1	Revisions sicheres Landespolizei-Informationssystem?.....	33
3.3.2	Aufzeichnung von Telefongesprächen bei der Polizei	34
3.3.3	Der anonyme Anruf – ZEVIS-Abrufe nicht immer nachprüfbar.....	36
3.3.4	Polizeiakten im Müllcontainer.....	37
3.3.5	Terrorismusbekämpfungsgesetz	38
3.3.6	Rasterfahndung	41
3.3.7	Polizeiliche Datenverarbeitung nicht geheim	44
3.4	VERKEHR	48
3.4.1	Rund ums Knöllchen – Datenverarbeitung in Bußgeldstellen.....	48
3.4.2	Videoaufzeichnungen im Rahmen der Verkehrsüberwachung.....	50

3.4.3	Straßenbenutzungsgebühren	52
3.5	VERFASSUNGSSCHUTZ	55
3.5.1	Novellierung des Landesverfassungsschutzgesetzes	55
3.6	EINWOHNERWESEN	57
3.6.1	Melderechtsrahmengesetz.....	57
3.6.2	Probleme mit dem Widerspruchsrecht bei Meldebehörden.....	58
3.7	KOMMUNALES	61
3.7.1	Zweckbindung von Daten gilt auch für Gemeindevertreter	61
3.7.2	Veröffentlichungen in der Gemeinde.....	62
3.7.3	Umgang mit personenbezogenen Daten bei Rechnungsprüfungen	64
3.7.4	Einbruch im Rechnungsprüfungsamt.....	65
3.8	STATISTIK	67
3.8.1	Empfehlungen zur Ausgestaltung einer Dienstanweisung für die kommunale Statistikstelle	67
3.8.2	Wann wird die Hochbaustatistik datenschutzgerecht?	68
3.9	TELEKOMMUNIKATION UND MEDIEN	69
3.9.1	Telekommunikations-Überwachungsverordnung.....	69
3.9.2	Evaluierung der Telekommunikationsüberwachung	69
3.9.3	Neue Medienordnung.....	70
3.9.4	Datenübermittlung für die Rundfunkgebührenfinanzierung.....	71
3.9.5	Konvention über Datennetzkriminalität.....	72
3.10	FINANZWESEN	74
3.10.1	Pannen bei der Elektronischen Steuererklärung	74
3.10.2	Fremdenverkehrsabgabe	75
3.10.3	Nutzung von Hundesteuerdaten für ordnungsbehördliche Zwecke?.....	76
3.10.4	PROfiskal	77
3.10.5	Was darf das Finanzamt über das private Telefonieren oder Surfen am Arbeitsplatz wissen?	79

3.11	SOZIALES.....	81
3.11.1	Umgang mit Sozialdaten – immer wieder aktuell.....	81
3.11.2	Auszahlung der Vertriebenenenzuwendung	83
3.11.3	Regelung zur Datenübermittlung zwischen Ärzten in der gesetzlichen Krankenversicherung	83
3.11.4	Behandlungsdaten an die Unfallkasse?.....	85
3.11.5	Dürfen Sanitätshäuser Gesundheitsdaten ihrer Kunden erheben und übermitteln?	86
3.11.6	Nachweis des sozialen Status für eine ermäßigte Eintrittskarte	88
3.11.7	Risikostrukturausgleich in der gesetzlichen Krankenversicherung	89
3.12	GESUNDHEITSWESEN	91
3.12.1	Innovatives Gesundheitsnetz Mecklenburg-Vorpommern	91
3.12.2	Mustervertrag zum Umgang mit personenbezogenen Daten im Auftrag	92
3.12.3	Wer darf einen Krankenhausentlassungsbericht erhalten?	93
3.12.4	Datenerhebung bei der Einschulungsuntersuchung	94
3.12.5	Einwilligung zur Speicherung im klinischen Krebsregister	95
3.12.6	Novellierung des Landeskrankenhausgesetzes	98
3.13	PERSONALWESEN	101
3.13.1	Personaldaten im Datennetz.....	101
3.13.2	Aktennotiz zur Vorbereitung eines Gesprächs	102
3.13.3	Elektronische Aufzeichnung von Personalgesprächen?	104
3.13.4	Keine Offenbarungspflicht bei Fragen nach bereits getilgten Straftaten	105
3.13.5	Einsicht in Personalunterlagen für potentielle Käufer	106
3.14	BILDUNG, KULTUR, WISSENSCHAFT UND FORSCHUNG.....	108
3.14.1	Sicherheit für die personenbezogenen Daten im Bildungsministerium....	108
3.14.2	Datenübermittlung bei Fernleihen	111
3.14.3	Datenschutzgerechte Nutzung des Archivgutes.....	111
3.14.4	Evaluation an den Hochschulen.....	112
3.15	WIRTSCHAFT UND GEWERBE.....	114
3.15.1	Einwilligungserklärung bei der Beantragung von Mitteln zur Ausbildungsplatzförderung.....	114

3.15.2	Videoüberwachung von Hauseingängen.....	115
3.15.3	Umgang mit Kundendaten bei einer Sparkasse	116
3.16	LAND-, FORST- UND WASSERWIRTSCHAFT	119
3.16.1	Bekanntgabe landwirtschaftlicher Betriebe beim Auftreten von BSE	119
3.17	E-GOVERNMENT	121
3.17.1	Datenschutzfreundlicher Service in der Verwaltung	121
3.17.2	Der rechtliche Rahmen für E-Government	122
3.17.3	Elektronische Signatur – bald auch in der Verwaltung Mecklenburg- Vorpommerns?.....	124
3.17.4	Wie sollten sich Behörden im Internet präsentieren?	126
3.17.5	Datenschutzaspekte von elektronischen Verzeichnisdiensten	128
3.17.6	Internet- und E-Mail-Nutzung am Arbeitsplatz.....	129
3.18	TECHNIK UND ORGANISATION	131
3.18.1	Das Corporate Network der Landesregierung	131
3.18.2	Die TK-Anlage der Landesregierung.....	132
3.18.3	Telearbeit – woran man denken sollte	135
3.18.4	Ein Personalcomputer in mehreren Netzen?.....	136
3.18.5	Prüfkriterien für datenschutzfreundliche Produkte	139
3.18.6	Open-Source-Software datenschutzfreundliche Technologie?.....	140
3.18.7	Drahtlose Vernetzung – noch nicht zu empfehlen	142
3.18.8	Datenschutzfreundliche Videoüberwachung?	143
4	FORTSETZUNG VON THEMEN FRÜHERER TÄTIGKEITSBERICHTE	147
4.1	Mitteilungen über Ausschlüsse vom Wahlrecht	148
4.2	Elektronisches Grundbuch	148
4.3	Wenn der Staatsanwalt zu Hause arbeitet.....	149
4.4	Ausübung des gemeindlichen Vorkaufsrechts.....	149
4.5	Data Warehouse	150
4.6	Volkszählung	151
4.7	Öffentliche Auslegung von Wählerverzeichnissen.....	152
4.8	INPOL-neu.....	153

4.9	Novellierung des Sicherheits- und Ordnungsgesetzes (SOG M-V)	154
4.10	Die neue Telekommunikations-Datenschutzverordnung.....	155
5	ARBEITSKREIS „TECHNISCHE UND ORGANISATORISCHE DATENSCHUTZFRAGEN“ (AK TECHNIK).....	157
6	ÖFFENTLICHKEITSARBEIT.....	161
7	ANLAGEN.....	165
8	ABKÜRZUNGSVERZEICHNIS	239
9	STICHWORTVERZEICHNIS	247
10	PUBLIKATIONEN.....	263

1. **EINLEITUNG**

Die letzten beiden Jahre brachten viele Veränderungen für den Datenschutz mit sich – jedoch nicht immer zugunsten des Bürgers und seines Rechts auf informationelle Selbstbestimmung.

So sind unter dem Eindruck der Terroranschläge am 11. September 2001 in den USA mit dem Terrorismusbekämpfungsgesetz schnell und überhastet Änderungen in fast zwanzig Gesetzen vorgenommen worden, die mit teilweise erheblichen Eingriffen in das Recht auf informationelle Selbstbestimmung verbunden sind. Die zum Teil schwierigen Rechtsfragen wurden in der Öffentlichkeit nicht ausreichend diskutiert. Unter den Regelungen sind auch solche, die nicht unmittelbar für die Bekämpfung des Terrorismus geeignet sind, sondern vielmehr auf langfristige Sicherheitsmaßnahmen abzielen, wie die Aufnahme biometrischer Merkmale in Ausweise und Pässe (3.3.5).

Der Innenminister unseres Landes hat als Folge dieser schrecklichen Ereignisse die Rasterfahndung angeordnet, ohne vorab jedoch alle rechtlichen Fragen ausreichend zu klären. Bei einer solchen umfangreichen Ermittlungsmethode ist jedoch von besonderer Bedeutung, dass die rechtlichen Rahmenbedingungen genauestens eingehalten werden. Ein wesentlicher Punkt bei der weiteren Begleitung der Rasterfahndung durch mich wird sein, darauf zu achten, dass die nicht mehr benötigten Datenbestände frühzeitig gelöscht werden (3.3.6).

Es gab aber auch positive Veränderungen im Datenschutz. Beispielsweise ist das Bundesdatenschutzgesetz novelliert worden, das nun unter anderem ein Gebot zur Datenvermeidung und zur Datensparsamkeit enthält (3.2.2). Seit Ende 2000 haben auch die Organe und Einrichtungen der Europäischen Gemeinschaft ein eigenes Datenschutz“gesetz“ – die EG-Datenschutzverordnung (3.2.3). Ebenfalls neu sind die detaillierten Regelungen der Charta der Europäischen Union, welche dem Datenschutz einen hohen Stellenwert einräumt (3.2.4). Bleibt zu hoffen, dass nach diesen positiven Änderungen des Datenschutzrechtes auch unser neues Landesdatenschutzgesetz, in dem nun endlich die EG-Datenschutzrichtlinie umgesetzt werden soll, die eine oder andere Regelung enthalten wird, die der modernen Entwicklung des Datenschutzrechtes hinreichend Rechnung trägt. Zurzeit wird der Novellierungsentwurf in den Ausschüssen behandelt. Die parlamentarische Beratung wird Anfang des Jahres 2002 fortgesetzt werden (3.2.1).

Bereits novelliert worden ist im Berichtszeitraum das Sicherheits- und Ordnungsgesetz des Landes (SOG M-V). Mit neuen Bestimmungen zu den verdachts- und ereignisunabhängigen Personenkontrollen sowie zur polizeilichen Überwachung von Wohnungen und Datenerhebungen aus dem Bereich geschützter Vertrauensverhältnisse sind die verfassungsrechtlichen Vorgaben weitgehend umgesetzt worden.

Die Datenübermittlung an private Stellen wurde gelockert und geht damit vergleichsweise weit über die Regelungen der Polizeigesetze anderer Länder hinaus (4.9).

Und auch das Landesverfassungsschutzgesetz ist mit einer Reihe von neuen Regelungen verabschiedet worden. Neben einigen datenschutzrechtlich bedenklichen Bestimmungen, wie einer nicht normenklaren Regelung zur Erweiterung der Befugnisse sowie der ausgeweiteten Erhebungsbefugnis bei Dritten, sind auch wesentliche Verbesserungen aufgenommen worden, so die abschließende Aufzählung der nachrichtendienstlichen Mittel zur heimlichen Informationsbeschaffung und die nachträgliche Unterrichtung von Betroffenen über das heimliche Mithören und Aufzeichnen des nicht öffentlich gesprochenen Wortes unter Einsatz technischer Mittel außerhalb von Wohnungen. Leider wurde nicht für alle verdeckten Maßnahmen eine solche Mitteilungspflicht in das Gesetz aufgenommen, was im Hinblick auf die Rechtsgarantie jedoch wünschenswert gewesen wäre (3.5.1).

Zu einem ganz anderen Thema: Die Videoüberwachung im Alltag nimmt zu. Viele Bürger nahmen dies zum Anlass und wandten sich mit einer Reihe datenschutzrechtlicher Fragen an mich. So interessierte die Bürger beispielsweise der Einsatz der Videotechnik bei der Verkehrsüberwachung, bei der Überwachung von Hauseingängen oder des Geschehens in Fahrzeugen des öffentlichen Nahverkehrs. Aber nicht nur die Bürger, auch die öffentlichen Stellen des Landes sind zunehmend für dieses Thema sensibilisiert und haben mich um Beratung bei dem Einsatz von Videotechnik gebeten. Selbst wenn der Einsatz einer einzelnen Videokamera sinnvoll und nützlich erscheinen mag, so darf nicht übersehen werden, dass jede einzelne Kamera ein weiterer Schritt zu einer flächendeckenden Überwachungsinfrastruktur ist. Die Leistungsfähigkeit der modernen Videotechnik lässt nur erahnen, mit welchen Überwachungsmöglichkeiten künftig zu rechnen ist. Eine „datenschutzfreundliche Videoüberwachung“ wird es auch in Zukunft nicht geben. Durch technische Maßnahmen ist es jedoch möglich, die Beeinträchtigung der Privatsphäre zu reduzieren (3.18.8).

Auch in diesem Berichtszeitraum habe ich in etlichen Bereichen der Polizei datenschutzrechtliche Mängel feststellen müssen. So sind beispielsweise sensible Unterlagen einer Polizeistation in einem Müllcontainer entsorgt worden (3.3.4). Aufgrund eines zunächst unentdeckt gebliebenen Softwarefehlers und durch die dann mit einer gezielten Programmierung einer Telefonanlage herbeigeführte generelle Zwangsaufzeichnung von Telefongesprächen ist rechtswidrig in das Fernmeldegeheimnis eingegriffen worden (3.3.3). Ein Fall geheimer polizeilicher Datenverarbeitung stimmte im Hinblick auf die Bindung der öffentlichen Stellen an die Grundrechte äußerst bedenklich. Hier musste ich mich mit widersprüchlichen Auskünften und einem Ver-

stoß des Landeskriminalamtes Mecklenburg-Vorpommern gegen datenschutzrechtliche Bestimmungen befassen (3.3.7).

Erfreulich ist dagegen die Entwicklung im Bereich der Kommunikationssicherheit. In meinem letzten Bericht hatte ich noch Rahmenbedingungen für den Einsatz kryptographischer Verfahren gefordert, mit deren Hilfe sensible Daten in verschlüsselter Form sicher übermittelt werden können. Das Justizministerium unterstützte mich bei meiner Forderung. Das Engagement des Ministeriums führte unter anderem zu dem Projekt „Digitale Signatur und Verschlüsselung“, in dem die Rahmenbedingungen für die Einführung von Verschlüsselungs- und Signaturverfahren in der Landesverwaltung erarbeitet werden sollen (3.17.3).

Die Sicherheit der Daten spielt auch beim Aufbau des Corporate Network der Landesverwaltung eine entscheidende Rolle (3.18.1). Für dessen Planung und Konzeption ist die Koordinierungs- und Beratungsstelle der Landesregierung für Informations- und Telekommunikationstechnik in der Landesverwaltung (LKSt) im Innenministerium zuständig. Diese erarbeitete mit dem künftigen Betreiber, der DVZ M-V GmbH, ein Feinkonzept und ein IT-Sicherheitsrahmenkonzept, bei deren Beratungen ich einbezogen worden bin. Die Konzepte sind mittlerweile gereift und enthalten konkrete Aussagen zu sicherheitstechnischen Anforderungen. Ein wichtiger Baustein im Corporate Network ist die zentrale Firewall, die den Übergang zum Internet und zwischen den Ressorts sichert. Nachdem die Ressorts begannen, diese zentrale Sicherheitseinrichtung zu nutzen, wurde das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit deren Prüfung beauftragt. Das BSI entdeckte einige technische Schwachstellen an der Firewall. Es spricht jedoch für das gewachsene Sicherheitsbewusstsein in der Landesverwaltung, dass alle Lücken verhältnismäßig schnell geschlossen werden konnten. Die gewählte Architektur erwies sich als leistungsfähig und sicher.



**SITUATION
DES DATENSCHUTZES**

Die ungestüme Entwicklung der Informations- und Kommunikationstechnik – insbesondere die starke Verbreitung des Internet – hat dazu geführt, dass dem Schutz personenbezogener Daten weltweit mehr Aufmerksamkeit geschenkt wird. Letztlich ist es vor allem dieser Entwicklung geschuldet, dass in den vergangenen zwei Jahren auch in der Bundesrepublik Deutschland zunehmende Aktivitäten zur Stärkung des Rechts auf informationelle Selbstbestimmung zu konstatieren sind. So war es unter anderem erforderlich geworden, das Datenschutzrecht im Bund und in den Ländern zu überarbeiten, es insbesondere auch dem Stand der Technik anzupassen. In einigen Ländern ist dies im Zusammenhang mit der Umsetzung der europäischen Datenschutzrichtlinie in nationales Recht bereits geschehen. Dort wurden die aus den siebziger Jahren stammenden Regelungen, die konkrete technische und organisatorische Maßnahmen beschrieben, durch moderne zielorientierte Bestimmungen ersetzt. In anderen Ländern und auch im Bund steht dieser Schritt noch aus.

Und ein weiterer positiver Trend zeichnet sich bei der Überarbeitung des Datenschutzrechts ab: Einige Länder haben die Gelegenheit wahrgenommen, die für den Bürger kaum verständliche Trennung der Datenschutzkontrolle in eine für den öffentlichen und eine für den nicht-öffentlichen Bereich zuständige Stelle aufzuheben und für alle Fragen des Datenschutzes eine Anlaufstelle im Land zu schaffen. Mecklenburg-Vorpommern schließt sich jedoch mit seinem Regierungsentwurf für ein neues Landesdatenschutzgesetz dieser Entwicklung nicht an. So müssen sich unsere Bürgerinnen und Bürger nach wie vor an das Innenministerium unseres Landes wenden, wenn beispielsweise eine Bank oder ein privates Krankenhaus nicht sorgsam mit ihren personenbezogenen Daten umgeht. Handelt es sich bei dem Geldinstitut jedoch um eine Sparkasse und bei dem Krankenhaus um eine kommunale Einrichtung, ist der Landesbeauftragte für den Datenschutz zuständig.

Es ist wohl nötig, künftig mehr darauf zu achten, dass es beim Datenschutz in erster Linie um den Bürger und sein Grundrecht und nicht primär um die Interessen der Behörden geht. Wie leicht der Bürger und sogar unsere Landesverfassung aus dem Blickfeld geraten können, zeigt ein Antrag im Rahmen der Novellierung unseres Landesdatenschutzgesetzes. Dort wurde gefordert, dass der Landesbeauftragte für den Datenschutz personenbezogene Daten, „die einem Berufs- oder besonderen Amtsgeheimnis ...“ unterliegen, nicht mehr kontrollieren darf. Nach unserer Landesverfassung kann sich aber jeder Bürger an den Datenschutzbeauftragten wenden, wenn er annimmt, dass die öffentliche Verwaltung sein Recht auf Schutz seiner Daten verletzt. Wenn dieses Recht keine Farce sein soll, dann muss der Datenschutzbeauftragte auch etwas für den Bürger tun können. Das Mindeste, was er tun kann, ist die Kontrolle des Umgangs mit den Daten bei der öffentlichen Stelle. Die Kontrollen des Landesbeauftragten für den Datenschutz sind nicht Selbstzweck, ebenso wenig wie die

Berufs- und Amtsgeheimnisse. Beides dient allein dem Schutz des Bürgers beim Umgang mit seinen Daten. Das hatte der Antragsteller offensichtlich nicht bedacht. Der Antrag wurde abgelehnt.

Nach den Terroranschlägen vom 11. September 2001 in den USA ist vieles anders – auch für den Datenschutz. Wenn auch spontane, direkte Schuldzuweisungen erfreulicherweise ausblieben, so war doch von einigen recht schnell ausgemacht, dass wir uns in Deutschland offensichtlich zuviel Datenschutz geleistet hätten. So verwundert es denn auch gar nicht, dass neben Altbekanntem wie „Datenschutz darf nicht zum Täterschutz verkommen“ neue Parolen wie „Menschenschutz geht vor Datenschutz“ in die Welt gesetzt wurden. Das leuchtet vordergründig vielen erst einmal ein, und es sitzt – insbesondere angesichts der schrecklichen Ereignisse. Landauf und landab muss der Datenschützer nun lang und breit erklären, dass Datenschutz und Menschenschutz nichts Gegensätzliches sind. Datenschutz ist Menschenschutz – was denn sonst? Dem Gesetzgeber von Mecklenburg-Vorpommern war das völlig klar, als er unser Landesdatenschutzgesetz schuf. Es heißt deshalb auch nicht „Gesetz zum Schutz der Daten ...“, sondern „Gesetz zum **Schutz des Bürgers** beim Umgang mit seinen Daten“.

Natürlich muss man nach dem 11. September etwas tun. Schnell muss etwas geschehen und langfristig wirksam muss es sein. Da sind Aufgeregtheit und platte Parolen wenig hilfreich.

Die Datenschutzbeauftragten des Bundes und der Länder waren sich von Anfang an darin einig, dass es erforderlich ist, auch in Deutschland massiv und mit geeigneten Maßnahmen auf die Herausforderungen des 11. September zu reagieren (Entschließung vom 1. Oktober 2001, Anlage 20). Mit der Rasterfahndung, dem Großen Lauschangriff, der Schleierfahndung, dem Abhören von Telefongesprächen und vielen weiteren, schon seit Jahren bestehenden Befugnissen der Sicherheitsbehörden waren die rechtlichen Voraussetzungen hierfür längst geschaffen. Trotzdem wurden mit dem Terrorismusbekämpfungsgesetz (siehe auch Punkt 3.3.5), das der Bundestag am 14. Dezember 2001 verabschiedet und dem der Bundesrat am 20. Dezember 2001 zugestimmt hat, in aller Eile die Befugnisse für die Geheimdienste und die Polizei noch einmal erweitert. Nicht alles davon scheint geeignet, den international agierenden Terrorismus schnell und wirksam zu bekämpfen; aber alles schränkt das Recht der Bürger auf informationelle Selbstbestimmung noch weiter ein. In Anbetracht dieser Tatsache stimmt es sehr bedenklich, wie schnell und glatt das Gesetzgebungsverfahren abgelaufen ist – zumal viele der nunmehr möglichen Maßnahmen ohnehin nicht kurzfristig realisiert werden können.

Bei einigen Maßnahmen entsteht sogar der Eindruck, dass die tragischen Ereignisse als „günstige“ Gelegenheit genommen wurden, um Regelungen, die seit langem vorbereitet in Schubladen lagen, nunmehr leicht in ein Terrorismusbekämpfungspaket mit einzubringen, beispielsweise die Speicherung biometrischer Merkmale in deutschen Personalausweisen und Pässen. Vor dem 11. September war noch völlig klar, dass diese Dokumente weder Fingerabdrücke noch verschlüsselte Angaben enthalten dürfen. Diese aus gutem Grunde gesetzlich fixierten Verbote werden nun durch das Terrorismusbekämpfungsgesetz schlagartig aufgehoben. Damit rückt die Möglichkeit eines einheitlichen Personenkennzeichens in eine bedrohliche Nähe.

Erinnern wir uns: In der DDR enthielt der Personalausweis eine Personenkennzahl (PKZ). Sie war nicht nur zentraler Suchbegriff für die Staatssicherheit, um Bürger in allen möglichen Dateien eindeutig zu identifizieren und auszuforschen. Auch unverdächtige öffentliche Stellen bedienten sich gerne der PKZ. So kam es durchaus vor, dass man bei einem persönlichen Anliegen in einem Amt weder nach seinem Namen noch nach seinem Geburtsdatum, sondern nur noch nach seiner PKZ gefragt wurde. Geht die Entwicklung wieder in diese Richtung? Denn nach dem Terrorismusbekämpfungsgesetz ist es nun nicht mehr verboten, ein ganzes Volk sogar daktyloskopisch zu behandeln, also von jedem Bürger zur Identifikation einen Fingerabdruck zu speichern. Eine solche Behandlung war bisher einzelnen Personengruppen, beispielsweise Straftätern, vorbehalten. Ohnehin ist nicht zu erkennen, was die biometrischen Merkmale in Ausweisen und Pässen mit der Bekämpfung des internationalen Terrorismus zu tun haben. Das Mindeste wäre doch, dass auch andere Länder vergleichbare Ausweisdokumente einführen. Weshalb sollte sich ein international agierender Terrorist ausgerechnet eines deutschen Ausweises oder Passes bedienen wollen, wo diese doch heute schon mit zu den fälschungssichersten zählen?

Bereits 1997 hatte der Bundesrat vergeblich versucht, Sicherheitsbehörden den Einsatz des so genannten IMSI-Catchers zu erlauben (siehe Dritter Tätigkeitsbericht, Punkt 3.18.1). Mit diesem Gerät ist die Ermittlung des Standortes eines Mobiltelefons, die Zuordnung der Gerätekennung zur Anschlussnummer und somit das Abhören von Mobilfunkgesprächen möglich. Vor dem Hintergrund der Terrorismusbekämpfung ist nun doch für das Bundesamt für Verfassungsschutz eine Befugnisnorm für den Einsatz des IMSI-Catchers geschaffen worden. Dieser darf eingesetzt werden, wenn andere Überwachungsmaßnahmen aussichtslos sind oder wesentlich erschwert wären. Dabei wurde allerdings nicht berücksichtigt, dass die oben genannten Funktionen des IMSI-Catchers nur für Mobiltelefone mit solchen Karten möglich sind, die von auskunftsverpflichteten – also deutschen – Telekommunikationsunternehmen ausgegeben worden sind. Für die gerade im Umfeld des internationalen Terrorismus naheliegende Nutzung ausländischer Anbieter ist der Einsatz des IMSI-Catchers deshalb wirkungslos.

Darüber hinaus ist zu berücksichtigen, dass das Gerät zur massiven Störung der gesamten Mobilkommunikation im Bereich seiner Reichweite führt, also eine Vielzahl unbescholtener Bürger trifft.

Auch Möglichkeiten der Videoüberwachung sind nach dem 11. September verstärkt diskutiert worden. Einige Politiker forderten sofort, nun endlich in großem Umfang Innenstädte, Flughäfen und Bahnhöfe zu überwachen, um potentielle Terroristen aufspüren zu können. Völlig unklar blieb bei diesen Forderungen jedoch, nach welchen Kriterien denn gesucht werden solle.

Alles in allem wurde im Zusammenhang mit der Terrorismusbekämpfung wieder einmal der Ruf nach weiteren technischen Überwachungsmaßnahmen lauter. Ob jedoch eine verstärkte Videoüberwachung, der Einsatz des IMSI-Catchers oder die Aufnahme biometrischer Merkmale in Pässe und Personalausweise überhaupt einen angemessenen Beitrag zur Bekämpfung des internationalen Terrorismus leisten können, ist äußerst fragwürdig. Grundsätzlich sollte nur das erlaubt werden, was geeignet, erforderlich und angemessen ist. Und wenn wir in der Zukunft nicht unversehens in einem Überwachungsstaat aufwachen wollen, dann müssen wir wohl heute schon verstärkt darauf achten, dass nicht jede der vorhandenen technischen Möglichkeiten zur Überwachung der Bürger genutzt wird. Anderenfalls könnte das Grundrecht auf informationelle Selbstbestimmung in seinem Wesensgehalt derart ausgehöhlt werden, dass es seine Schutzwirkung verliert. Daher ist es an der Zeit, wieder mit Augenmaß auf die Gefahren für unseren demokratischen Rechtsstaat zu reagieren, ohne dabei die Existenz elementarer Menschenrechte zu gefährden.

Eigentlich darf der Bürger erwarten, dass die vielen Befugnisserweiterungen für die Geheimdienste und andere Sicherheitsbehörden mit einer Erweiterung der Befugnisse und Kapazitäten der Kontrollbehörden einhergehen. Davon ist gegenwärtig nichts zu erkennen. Ebenso wäre es dringend erforderlich, das Recht des Bürgers auf Zugang zu Informationen bundesweit zu regeln. Noch ist dieses Recht nur in wenigen Ländern gesetzlich verankert. Und es ist wohl höchste Zeit, dass der Bürger sein Grundrecht auf informationelle Selbstbestimmung – so klargestellt vom Bundesverfassungsgericht im Volkszählungsurteil von 1983 – auch ausdrücklich im Grundgesetz wiederfindet.

3.

**SORGEN DER BÜRGER,
EINZELFÄLLE, BERATUNGEN,
KONTROLLEN, STELLUNGNAHMEN,
GESETZE, VERORDNUNGEN**

3.1 Rechtswesen

3.1.1 Strafverfahrensänderungsgesetz

Am 2. August 2000 ist das Strafverfahrensänderungsgesetz verabschiedet worden. Die Hinweise der Datenschutzbeauftragten des Bundes und der Länder aus ihrer Entschließung vom 14./15. März 2000 wurden nicht berücksichtigt (siehe Anlage 4). Die folgenden Beispiele verdeutlichen, dass es trotz einer jahrzehntelangen Diskussion nicht zu dem verfassungsrechtlich gebotenen Ausgleich zwischen dem Persönlichkeitsschutz des Einzelnen und den Interessen der Strafverfolgungsbehörden gekommen ist.

- Nunmehr ist es beispielsweise möglich, dass Zeuginnen und Zeugen auch bei Straftaten von nicht erheblicher Bedeutung durch Öffentlichkeitsfahndung im Fernsehen oder im Internet gesucht werden.
- Die Zweckbindung von Daten aus der Gefahrenabwehr und der Strafverfolgung wird nahezu aufgehoben. Damit werden die landespolizeirechtlichen Vorschriften zur Wahrung der Zweckbindung und damit die Kompetenzen des Landesgesetzgebers unterlaufen.
- Verfahrensdaten dürfen auch zur Verfolgung künftiger Straftaten in staatsanwaltlichen Informationssystemen gespeichert werden, obwohl bei der Polizei gleichartige Dateien auf landesrechtlicher Grundlage bereits seit langem geführt werden.
- Schon allein bei „berechtigtem Interesse“ bekommen nun am Verfahren nicht beteiligte Personen Einsicht in sensible Strafverfahrensakten.

Die Interessen der Strafverfolgungsbehörden hatten bei der Gestaltung dieses Gesetzes eindeutig Vorrang vor den Persönlichkeitsrechten von Betroffenen.

3.1.2 Nachfolgeregelung zu § 12 FAG

Die Bundesregierung hat im September 2001 einen Gesetzentwurf zur Änderung der Strafprozessordnung eingebracht (BR-Drs. 702/01). Er behandelt die Nachfolgeregelung zu § 12 des Gesetzes über Fernmeldeanlagen (FAG), der mit Ablauf des 31. Dezember 2001 außer Kraft trat.

§ 12 FAG gestattete den Strafverfolgungsbehörden, von den Telediensteanbietern Auskunft über Verbindungsdaten vergangener und nach umstrittener Rechtsprechung sogar künftiger Telekommunikationsvorgänge unabhängig von der Schwere der Straftat zu verlangen. Diese rechtliche Grundlage stammt jedoch noch aus einer Zeit, in der die analoge Vermittlungstechnik vorherrschte und nicht für jedes Gespräch personenbezogene Verbindungsdaten erzeugt wurden. Im Zeitalter der Digitaltechnik jedoch, in dem Daten vollständig erfasst und damit Verhaltensprofile gebildet werden können, verstößt § 12 FAG gegen den Verhältnismäßigkeitsgrundsatz und ist somit nicht mehr geeignet, derartige Eingriffe in das Telekommunikationsgeheimnis zu rechtfertigen.

Dies haben die Datenschutzbeauftragten des Bundes und der Länder bereits auf ihrer 58. Konferenz am 7./8. Oktober 1999 in einer Entschließung deutlich gemacht (siehe Vierter Tätigkeitsbericht, Anlage 19). Auf der 59. Konferenz am 14./15. März 2000 haben wir erneut an den Gesetzgeber appelliert, die Eingriffsbefugnisse unter Beachtung der grundrechtlichen Bindungen und Anforderungen neu festzulegen (siehe Anlage 5). Und es wurde gefordert, die Neuregelung in Abstimmung mit § 100a Strafprozessordnung (StPO) in diesem Gesetz anzusiedeln, da die gesetzliche Ermächtigung für den Zugriff auf Verbindungsdaten sachlich in die Strafprozessordnung gehört.

Die Bundesregierung ist mit ihrem Gesetzentwurf für die Neuregelung zu § 12 FAG, der eine Reihe datenschutzrechtlich positiver Ansätze enthält, den Forderungen nur teilweise nachgekommen. Während des laufenden Gesetzgebungsverfahrens habe ich deshalb gegenüber unserem Justizministerium auf folgende Regelungen im Entwurf hingewiesen, die bislang nicht den datenschutzrechtlichen Anforderungen entsprechen:

- IMEI-Nummern (Gerätekennzeichnung bei Mobiltelefonen) sollten entgegen der Absicht des Gesetzentwurfes nicht als Telekommunikationsverbindungsdaten an die Strafverfolgungsbehörden übermittelt werden, da sie nicht in den gemäß Teledienstedatenschutzgesetz (TDDSG) und Telekommunikationsdatenschutzverordnung (TDSV) zulässigen Rahmen der Datenverarbeitung der Telekommunikationsanbieter fallen.
- Die gesetzliche Regelung zu den festen und den dynamischen IP-Adressen (Internet-Protokoll-Adressen) sollte im Hinblick auf eine Unterscheidung beider Adressen und die damit verbundenen unterschiedlichen Anforderungen an die Zugriffsbefugnisse konkretisiert werden. Die festen IP-Adressen sind Bestandsdaten

im Sinne von § 89 Abs. 6 Telekommunikationsgesetz (TKG) und können, ohne dass sie vom Vorbehalt der richterlichen Anordnung gemäß § 100g StPO erfasst werden, mitgeteilt werden. Bei den so genannten dynamischen IP-Adressen, die im Einzelfall und während des Kommunikationsvorganges jeweils an die Nutzer neu vergeben werden, handelt es sich dagegen um Verbindungsdaten im Sinne von § 2 Nr. 4 TDSV, deren Übermittlung an die Strafverfolgungsbehörden den höheren Anforderungen der §§ 100g, 100h StPO unterliegen muss. Diese Unterscheidung und ihre Rechtsfolgen für die Voraussetzung der Auskunftserteilung sind bislang nicht deutlich herausgearbeitet worden.

- Zum Schutz der Betroffenen sollte in § 100h StPO die Voraussetzung mit aufgenommen werden, dass es sich bei dem zustimmenden Betroffenen um einen verteidigten Beschuldigten handeln muss, damit Vor- und Nachteile einer Beweisverwertung für den Beschuldigten durch den Verteidiger besser abgewogen werden können. Mit dieser zusätzlichen Voraussetzung soll der Gefahr begegnet werden, dass der Beschuldigte nur deshalb der Verwendung seiner bislang erlangten personenbezogenen Daten zu Beweis Zwecken in anderen Strafverfahren zustimmt, um nicht wegen mangelnder Kooperationsbereitschaft benachteiligt zu werden.

Der Bundestag hat am 20. Dezember 2001 das Gesetz zur Änderung der Strafprozessordnung verabschiedet (BGBl. I S. 3879). Die genannten Empfehlungen wurden nicht berücksichtigt.

3.1.3 Parlamentarische Kontrolle von Lauschangriffen

Unzureichende Berichte der Bundesregierung

Die Bundesregierung hat den Bundestag jährlich über die nach Art. 13 Abs. 3 Grundgesetz (GG) zur Strafverfolgung durchgeführten Großen Lauschangriffe zu unterrichten (siehe Vierter Tätigkeitsbericht, Punkt 3.1.5). § 100e Strafprozessordnung (StPO) konkretisiert diese Berichtspflicht: Grundlage dafür sind Mitteilungen der Länder über Anlass, Umfang, Dauer, Ergebnis und Kosten der durchgeführten Lauschangriffe.

Inzwischen liegen die Berichte zur Überwachung von Wohnungen aus den Jahren 1998, 1999 und 2000 vor. Nach wie vor sind auch im Jahr 2000 die in den tabellarischen Übersichten dargestellten Maßnahmen der akustischen Wohnraumüberwachung unzureichend beschrieben.

Das Kontrollgremium des Deutschen Bundestages (Art. 13 Abs. 6 GG) hat die Konferenz der Justizministerinnen und -minister der Länder gebeten, diesem Sachverhalt nachzugehen. Im April 2001 hat die Konferenz ihren Strafrechtsausschuss mit entsprechenden Prüfungen beauftragt. Ungeachtet dieser Auswertungen bleibt die Forderung, dass die jährlichen Berichte der Bundesregierung deutlich an Aussagekraft zunehmen müssen, um eine effektive parlamentarische Kontrolle zu gewährleisten.

Parlamentarische Kontrolle von Lauschangriffen auf Landesebene

Die Länder haben nach Art. 13 Abs. 6 Satz 3 GG eine parlamentarische Kontrolle der Lauschangriffe zur Strafverfolgung und zur Gefahrenabwehr zu gewährleisten, die der auf Bundesebene gleichwertig ist. Den Landesparlamenten müssen jährlich entsprechende Berichte vorgelegt werden.

Mit dem Zweiten Gesetz zur Änderung des Sicherheits- und Ordnungsgesetzes vom 24. Oktober 2001 ist nunmehr eine Vorschrift eingeführt worden (§ 34 Abs. 7 S. 2 SOG M-V), wonach das Justizministerium das Gremium des Landtages, welches für die Kontrolle der Lauschangriffe im präventiven Bereich zuständig ist, auch über die nach § 100c Abs. 1 Nr. 3 StPO erfolgten Maßnahmen unterrichten muss. Damit ist die Forderung der Datenschutzbeauftragten nach einer gesetzlichen Regelung erfüllt worden.

3.1.4 Veröffentlichungen der Justiz im Internet

Insolvenzverfahren

Die Bundesregierung hat einen Gesetzentwurf verabschiedet, wonach Bekanntmachungen über Insolvenzverfahren künftig auch im Internet veröffentlicht werden dürfen (BT-Drs. 14/5680). Bisher wurden dafür der amtliche Anzeiger sowie Tageszeitungen genutzt. Ein maßgebliches Argument für die neue Verfahrensweise ist die damit verbundene Kostenersparnis für die Schuldner. Weitgehend unberücksichtigt blieben jedoch die damit verbundenen Gefährdungen für das Recht auf informationelle Selbstbestimmung dieser Personen. Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung vom 24. April 2001 darauf hingewiesen, dass Informationen im Internet für jedermann zugänglich sind und auch nach Abschluss des Insolvenzverfahrens von Dritten über diesen Zeitraum hinaus gespeichert und genutzt werden können, ohne dass hierauf eingewirkt werden kann (siehe Anlage 18).

Der wirtschaftliche Neubeginn eines Schuldners nach einem erfolgreich durchlaufenen Insolvenzverfahren wäre somit möglicherweise dauerhaft gefährdet.

Der Gesetzgeber hat diese Bedenken in seinen Beratungen zum Gesetzentwurf aufgegriffen und in § 9 Abs. 2 des Gesetzes zur Änderung der Insolvenzordnung und anderer Gesetze vom 26. Oktober 2001 (BGBl. I S. 2711) ergänzende Regelungen aufgenommen. Um den Gefährdungen für das Recht auf informationelle Selbstbestimmung wirksam zu begegnen, sollen nunmehr in einer Verordnung Einzelheiten zur Veröffentlichung im Internet geregelt werden. Das betrifft insbesondere Löschrufen sowie technische und organisatorische Maßnahmen, die die Integrität und die Authentizität der Daten gewährleisten sollen. Darüber hinaus hat der Deutsche Bundestag die Bundesregierung gebeten, bis zum Ende des Jahres 2001 zu prüfen, wie verhindert werden kann, dass Daten nach Ablauf der Löschrufenfrist weiter über das Internet veröffentlicht werden. Die Bundesregierung soll hierzu gegebenenfalls einen Gesetzentwurf bis zum 31. März 2002 vorlegen (BT-Drs. 14/6473). Zu einem Verordnungsentwurf des Bundesministeriums der Justiz über die nähere Ausgestaltung des neuen Verfahrens habe ich gegenüber unserem Justizministerium Empfehlungen gegeben. Wie das Verfahren künftig aussehen wird und ob den Gefährdungen für das Recht auf informationelle Selbstbestimmung wirksam entgegengewirkt werden kann, bleibt abzuwarten.

Zwangsversteigerungen

Seit einiger Zeit veröffentlichen Gerichte unseres Landes Zwangsversteigerungen im Internet. Dadurch soll ein größerer Verbreitungsgrad erreicht und somit ein weiterer Interessentenkreis angesprochen werden, was nicht zuletzt auch im Interesse des Schuldners liegt. Die Daten im Internet enthalten – im Gegensatz zu den Veröffentlichungen in den herkömmlichen Medien – keine Angaben zu den Eigentümern, so dass eine Zuordnung zu einer natürlichen Person nicht ohne weiteres möglich ist. Je nach Lage des Einzelfalles kann jedoch ein Personenbezug mit zusätzlichen Daten hergestellt werden.

In einem Fall waren beispielsweise die Mieter eines Einfamilienhauses betroffen. Das Versteigerungsobjekt war mit der Postanschrift sowie mit Fotografien von innen und außen dargestellt worden. Dritte konnten die Wohnungseinrichtung betrachten, und es war ihnen auch möglich, die Namen der Mieter beispielsweise über die Adresse des Einfamilienhauses und Einsicht in das Telefonbuch in Erfahrung zu bringen. Auf Veranlassung des Rechtsanwaltes der Betroffenen hat der Direktor des Amtsgerichtes die Fotografien der Wohnungseinrichtung wieder entfernen lassen.

Das Zwangsversteigerungsgesetz enthält keine Vorschriften zur Veröffentlichung personenbezogener Daten im Internet. Da eine solche Veröffentlichung jedoch aufgrund der weltweit fast unbegrenzten Möglichkeiten zur Kenntnisnahme und Auswertung der Daten eine neue datenschutzrechtliche Qualität darstellt, sollten hierfür auch bereichsspezifische Regelungen geschaffen werden. Das Justizministerium teilte mir hierzu mit, dass die Veröffentlichungspraxis im Internet und die damit möglicherweise auftretenden datenschutzrechtlichen Probleme bekannt seien. Es hatte seinerzeit bereits die Gerichte darauf hingewiesen und mein Schreiben zum Anlass einer nochmaligen Prüfung genommen. So bleibt abzuwarten, inwieweit dieser Bereich gesetzlich geregelt wird.

3.1.5 Novelliertes G 10-Gesetz

Das Bundesverfassungsgericht hat mit einer Entscheidung vom 14. Juli 1999 einige Bestimmungen des Gesetzes zu Artikel 10 Grundgesetz (GG) beanstandet, nach denen der Bundesnachrichtendienst strategische Überwachungen durchgeführt hat (siehe dazu EntschlieÙung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000, Anlage 1). Dem Gesetzgeber wurde eine Frist bis zum 30. Juni 2001 eingeräumt, um einen verfassungsmäßigen Zustand herzustellen.

In ihrer EntschlieÙung vom 8./9. März 2001 äußern die Datenschutzbeauftragten des Bundes und der Länder die Befürchtungen, dass

- die Befugnisse der Nachrichtendienste zur Übermittlung und Verwendung von G 10-Daten an Strafverfolgungsbehörden deutlich erweitert werden sollen, indem Erkenntnisse der Nachrichtendienste unter anderem zur Strafverfolgung weit über die Schwerekriminalität hinaus genutzt werden dürfen,
- künftig deutlich weniger Betroffene benachrichtigt werden,
- der Verzicht auf die Kennzeichnung von G 10-Daten sogar ohne vorherige Zustimmung der G 10-Kommission zulässig sein soll.

Am 26. Juni 2001 ist das Gesetz zur Neuregelung von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses (G 10-Gesetz) verabschiedet worden. Die Hinweise der Datenschutzbeauftragten wurden dabei nicht berücksichtigt. Es bleibt abzuwarten, inwieweit sie im Ausführungsgesetz zum G 10-Gesetz auf Landesebene Berücksichtigung finden.

3.2 Neues Datenschutzrecht

3.2.1 Die Novellierung des Landesdatenschutzgesetzes (DSG M-V)

Gegenwärtig wird der Kabinettsentwurf eines Datenschutzgesetzes vom 17. Juli 2001 in den Ausschüssen des Landtages behandelt. Die parlamentarische Beratung wird Anfang des Jahres 2002 fortgesetzt.

3.2.2 Novelliertes Bundesdatenschutzgesetz

Am 23. Mai 2001 trat das neue Bundesdatenschutzgesetz (BDSG) in Kraft. Die Novellierung diente vor allem der Umsetzung der EG-Datenschutzrichtlinie (siehe Vierter Tätigkeitsbericht, Punkt 2.4). Die Aufnahme des Gebots zur Datenvermeidung und zur Datensparsamkeit und die Einführung des Datenschutzaudits (Prüfung von Datenverarbeitungssystemen und Datenschutzkonzepten durch unabhängige Gutachter) sind dabei ausdrücklich zu begrüßen (siehe die Entschließung der Datenschutzbeauftragten vom 10. Oktober 2000, Anlage 7).

Leider wurden die Technikregelungen nur wenig überarbeitet. Sie sind nicht ziel-, sondern maßnahmeorientiert und stammen in ihrem Kern aus den siebziger Jahren (siehe dazu ausführlich Vierter Tätigkeitsbericht, Punkt 2.3). Des Weiteren ist das bisher schon schwer lesbare Gesetz durch das Aufpfropfen der neuen Bestimmungen teilweise kaum noch überschaubar und verständlich.

Die zweite Novellierungsstufe (siehe Vierter Tätigkeitsbericht, Punkt 2.2) soll diese Mängel abstellen sowie den Anforderungen der modernen, internationalen Informationsgesellschaft Rechnung tragen. Dazu hatte das Bundesministerium des Innern ein Gutachten zur „Modernisierung des Datenschutzrechts“ in Auftrag gegeben. Koordinator des dreiköpfigen Gutachtergremiums ist der Berliner Beauftragte für Datenschutz und Informationsfreiheit. Das am 12. November 2001 übergebene Gutachten enthält detaillierte Vorschläge für ein umfassendes allgemeines Datenschutzrecht, welches Spezialregelungen in bereichsspezifischen Gesetzen zur Ausnahme werden lässt, hohe Transparenz der Datenverarbeitung fordert und „Datenschutz durch Technik“ propagiert. Bei seiner Erstellung wurden auch Anregungen der Datenschutzbeauftragten des Bundes und der Länder berücksichtigt. Das Gutachten ist im Internet unter http://www.bmi.bund.de/dokumente/Bestellservice/ix_61638.htm abrufbar.

Es ist zu hoffen, dass auf der Basis dieses Gutachtens ein modernes Bundesdatenschutzgesetz, wenn schon nicht – wie ursprünglich geplant – zum Ende dieser, so doch zu Beginn der nächsten Legislaturperiode verabschiedet wird.

3.2.3 EG-Datenschutzverordnung

Seit Ende 2000 haben die Organe und Einrichtungen der EG ihr eigenes Datenschutz„gesetz“, die EG-Datenschutzverordnung. Sie ist zu unterscheiden von der EG-Datenschutzrichtlinie. Die Richtlinie wendet sich an die Mitgliedstaaten der EG und enthält datenschutzrechtliche Vorgaben, die diese Staaten in nationales Recht umsetzen müssen (siehe Dritter und Vierter Tätigkeitsbericht, jeweils Punkt 2.4). Auch die Organe und Einrichtungen der EG selbst sind Adressaten der Datenschutzrichtlinie.

Die EG-Datenschutzverordnung ist eine Rechtsvorschrift, mit der die EG die allgemeine Datenschutzrichtlinie und die ISDN/TK-Datenschutzrichtlinie der EG (siehe Dritter Tätigkeitsbericht, Punkt 3.10.1) für ihren eigenen Bereich umsetzt. Sie ist das Pendant zu den Datenschutzgesetzen der EG-Mitgliedstaaten und dient dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der EG.

Die Verordnung enthält unter anderem folgende Regelungen:

- Die Organe und Einrichtungen der EG dürfen personenbezogene Daten in der Regel nur an solche Staaten oder Organisationen außerhalb des Geltungsbereichs der Datenschutzrichtlinie übermitteln, die ein angemessenes Datenschutzniveau sicherstellen.
- Die Verarbeitung besonders sensibler personenbezogener Daten, wie Daten, aus denen die Herkunft oder religiöse Überzeugungen hervorgehen, dürfen nur in Ausnahmefällen verarbeitet werden.
- Die Sicherheit der Verarbeitung ist durch geeignete technische und organisatorische Maßnahmen zu gewährleisten. Allerdings übernimmt diese Bestimmung im Wortlaut meist die detaillierten Anforderungen der entsprechenden Regelung der deutschen Datenschutzgesetze vor deren Novellierung anlässlich der Umsetzung der Datenschutzrichtlinie. Sie muss daher als technisch überholt angesehen werden (siehe Vierter Tätigkeitsbericht, Punkt 2.3).

- Jedes Organ und jede Einrichtung der EG hat einen weisungsunabhängigen behördlichen Datenschutzbeauftragten zu bestellen. Zu seinen Aufgaben gehört es, die innerbehördliche Anwendung der Verordnung zu gewährleisten.
- Es wird eine unabhängige Kontrollbehörde, der Europäische Datenschutzbeauftragte, eingerichtet. Er berät und kontrolliert die Organe und Einrichtungen der EG bei der Verarbeitung personenbezogener Daten. Dazu werden ihm umfangreiche Befugnisse eingeräumt, insbesondere ein uneingeschränktes Zugangsrecht zu allen Räumlichkeiten, zu allen personenbezogenen Daten und zu allen für seine Untersuchungen erforderlichen Informationen der EG-Institutionen. Gegen die Entscheidungen des Europäischen Datenschutzbeauftragten kann Klage beim Europäischen Gerichtshof erhoben werden.
- Die betroffenen Personen haben Rechte auf Auskunft, Sperrung, Berichtigung und Löschung ihrer Daten sowie auf Beschwerde beim Europäischen Datenschutzbeauftragten. In besonderen Fällen haben sie ein Recht auf Widerspruch gegen an sich zulässige Verarbeitungen ihrer personenbezogenen Daten. Die Wahrnehmung dieser Rechte ist unentgeltlich.
- Automatisierte Einzelentscheidungen, die sich negativ für die Betroffenen auswirken können, sind nur zulässig, wenn Rechtsvorschriften sie erlauben oder der Europäische Datenschutzbeauftragte ausdrücklich zugestimmt hat und Maßnahmen zum Schutz der berechtigten Interessen der Betroffenen ergriffen worden sind.

Die Verordnung ist in einigen Punkten datenschutzfreundlicher als die Richtlinie. So ist der Auskunftsanspruch – wie auch im deutschen Datenschutzrecht üblich – kostenfrei, wohingegen die Richtlinie nur vorschreibt, dass keine „übermäßigen Kosten“ verlangt werden dürfen. Darüber hinaus enthält die Verordnung – im Gegensatz zu anderen Datenschutzvorschriften – ein eigenes Kapitel zum „Schutz der personenbezogenen Daten und der Privatsphäre im Rahmen interner Telekommunikationsnetze“.

3.2.4 EU-Grundrechte-Charta

Am 7. Dezember 2000 wurde in Nizza anlässlich der Tagung des Europäischen Rates, also der Staats- und Regierungschefs der EU-Mitgliedstaaten, die „Charta der Grundrechte der Europäischen Union“ verkündet.

Artikel 8 der Charta enthält detaillierte Regelungen zum Datenschutz. Die Datenschutzbeauftragten des Bundes und der Länder hatten in einer Entschließung auf ihrer 58. Konferenz am 7./8. Oktober 1999 die Einfügung eines Grundrechts auf Datenschutz gefordert (siehe Vierter Tätigkeitsbericht, 16. Anlage). Der zur Erarbeitung der Charta eingesetzte Konvent unter Leitung des ehemaligen Bundespräsidenten Roman Herzog setzte diese Forderung um und formulierte unter der Überschrift „Schutz personenbezogener Daten“ die folgenden Regelungen:

„(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Personen oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.“

Neben diesem Datenschutzgrundrecht garantiert Artikel 42 der Charta das „Recht auf Zugang zu Dokumenten“:

„Die Unionsbürgerinnen und Unionsbürger sowie jede natürliche oder juristische Person mit Wohnsitz oder satzungsmäßigem Sitz in einem Mitgliedstaat haben das Recht auf Zugang zu den Dokumenten des Europäischen Parlaments, des Rates und der Kommission.“

Die Charta hat zwar keine rechtsverbindliche Wirkung, dennoch ist sie von praktischer Bedeutung, da sie von den Organen der EG, insbesondere dem Europäischen Gerichtshof, bei der Rechtsanwendung berücksichtigt wird. Außerdem macht die Charta deutlich, dass die EU dem Datenschutz einen hohen Stellenwert einräumt, was nicht ohne Einfluss auf die einzelnen Mitgliedstaaten bleiben sollte.

3.3 Polizei

3.3.1 Revisions-sicheres Landespolizei-Informationssystem?

Bei der Bearbeitung von Petitionen im Zusammenhang mit dem Landesweiten Polizei-Informationssystem (LAPIS) (siehe auch Punkte 3.3.3 und 3.13.1) stellte ich Mängel bei der Protokollierung des Umgangs mit personenbezogenen Daten in diesem System fest. Um mir einen möglichst umfassenden Überblick über die Revisions-sicherheit der Datenverarbeitung in LAPIS zu verschaffen, habe ich im Januar 2001 eine Polizeistation und im März 2001 die entsprechenden Protokollierungskomponenten beim zentralen LAPIS Netz- und Systemmanagement (NSM) kontrolliert. Die Kontrolle sollte Aufschluss darüber geben, ob durch Protokollierung in den verschiedenen Verfahren polizeilicher Datenverarbeitung nachvollziehbar ist, wer wann welche Daten gelesen, eingegeben, verändert oder gelöscht hat.

Die Protokollierungskomponenten des Ordnungswidrigkeitenverfahrens (OWI) und der polizeilichen Erkenntnisdatei (PED) habe ich nicht geprüft, weil ich bereits frühzeitig in die Entwicklung und Tests einbezogen war und mir schon zum Zeitpunkt der Einführung von PED und OWI datenschutzgerechte Protokollierungs- und Auswerteverfahren demonstriert worden waren.

Ein großer Teil der polizeilichen Vorgangsbearbeitung wird durch den so genannten Elektronischen Vorgangsassistenten (EVA) unterstützt. Auch in diesem Bereich genügte die Protokollierung den datenschutzrechtlichen Anforderungen. Insbesondere die Kontrolle im NSM zeigte, dass es mit Hilfe einer speziellen Auswertesoftware mit relativ geringem Aufwand möglich ist, die einzelnen Schritte beim Bearbeiten der von EVA unterstützten Vorgänge nachzuvollziehen. Die Testabfragen, die Polizeibeamte während meines Besuches in der Polizeistation durchgeführt hatten, waren vollständig im Protokolldatenbestand dokumentiert.

Kritikwürdig war die Revisions-sicherheit bei der Verarbeitung von Personalakten-daten. Gerade in diesem Bereich werden hohe Anforderungen gestellt, weil die hier verarbeiteten personenbezogenen Daten besonders schutzwürdig sind. Der IT-Strukturrahmen des Landes sieht deshalb vor, eine eigens für diese Zwecke entwickelte Software zu verwenden. Bereits Mitte 1999 wurde das Elektronische Personal-, Organisations- und Stellenverwaltungssystem (EPOS) durch Kabinettsbeschluss zum Landesstandard erklärt. Diese Software erfüllt die wesentlichen Anforderungen an die Revisions-sicherheit. Die Kontrolle zeigte jedoch, dass EPOS im Bereich der Lan-

despolizei nicht eingesetzt wird. Personaldaten werden dort mit den Software-Produkten MS-Word und MS-Excel verarbeitet. Die Nutzeraktivitäten wurden lediglich im so genannten Journal von Outlook gespeichert und vom Betriebssystem MS Windows NT protokolliert. Den Anforderungen an eine wirksame Eingabekontrolle nach § 17 Abs. 2 Nr. 7 Landesdatenschutzgesetz von Mecklenburg-Vorpommern (DSG MV) werden diese Hilfsmittel jedoch nicht gerecht, weil derartige Protokolle sehr leicht zu manipulieren sind.

Der Innenminister hat meine Auffassung geteilt und zugesagt, die Einbindung von EPOS in LAPIS zu prüfen. Darüber hinaus hat er in Aussicht gestellt, die Personalaktendaten der Polizei ab 2002 mit dem Landesstandard EPOS zu verarbeiten. Um auch für den Übergangszeitraum eine reversionssichere Protokollierung zu gewährleisten, werden die Protokolldaten durch eine Zusatzsoftware an das zentrale NSM übertragen. Die Auswertung erfolgt dort mit einer speziellen Software. Nur noch ein ausgewählter Personenkreis hat Zugriff auf die Protokolle.

Ein weiterer Schwerpunkt meiner Kontrolle war die Protokollierung von Abrufen aus dem Zentralen Verkehrsinformationssystem (ZEVIS) (siehe auch Punkt 3.3.3). Es zeigte sich, dass ZEVIS-Abrufe nur dann zweifelsfrei dem Verursacher zugeordnet werden können, wenn die Abfrage während der Bearbeitung eines konkreten Vorgangs mit EVA erfolgt. Wird jedoch auf den ZEVIS-Datenbestand ohne Vorgangsbezug über PED oder mit Hilfe eines Terminalprogramms zugegriffen, kann nur auf das Terminal geschlossen werden, von dem die Anfrage abgesandt wurde. Der in Frage kommende Personenkreis kann durch Auswertung der Dienstpläne möglicherweise eingeschränkt werden, einem einzelnen Mitarbeiter wird die Recherche jedoch in den seltensten Fällen eindeutig zuzuordnen sein. Somit ist in allen Fällen, in denen keine erweiterte Protokollierung nach § 36 Abs. 7 Satz 1 Straßenverkehrsgesetz erfolgt, regelmäßig kein Rückschluss auf den Abfragenden und somit keine Prüfung der Rechtmäßigkeit von Abfragen möglich.

Der Innenminister hat mir mitgeteilt, dass dieser Mangel im Zusammenhang mit der bundesweiten Einführung des neuen Polizeiinformationssystems INPOL-neu abgestellt werden soll. Es ist vorgesehen, künftig bei jeder ZEVIS-Abfrage die verantwortliche Person und den Anlass der Abfrage zu protokollieren.

3.3.2 Aufzeichnung von Telefongesprächen bei der Polizei

Im Juli 2000 bin ich darüber informiert worden, dass in einer Polizeidirektion des Landes von Polizeibeamten geführte Telefongespräche in unzulässiger Weise zwangsaufgezeichnet wurden. Teile dieser Aufzeichnungen sollten in einem Disziplinarverfahren gegen einen Polizeibeamten verwendet werden.

Neben meiner rechtlichen Prüfung des Falls hatte die Polizeiabteilung des Innenministeriums im Januar 2001 die entsprechenden technischen Details in allen Polizeidirektionen kontrolliert. Dabei war festgestellt worden, dass an den Arbeitsplätzen der Leitstellen aller Polizeidirektionen der gleiche Softwarefehler auftrat. Dieser bewirkte, dass vom Bedientisch der Leitstelle geführte dienstliche und private Nebestellengespräche unter bestimmten Voraussetzungen mitgeschnitten werden konnten. Sofort nach Feststellung dieses Fehlers war eine Firma beauftragt worden, einen ordnungsgemäßen Zustand herzustellen.

Nachdem im Januar 2001 die Bedientische repariert waren, habe ich eine Polizeidirektion kontrolliert, um den Zustand der Dokumentationsanlage zu prüfen.

Während der Kontrolle wurde mir die vorherige Fehlfunktion nochmals detailliert erläutert. So genannte Drahtgespräche wurden am Bedientisch immer dann zwangsaufgezeichnet, wenn bei Beginn dieses Gespräches bereits ein Funkgespräch geführt wurde. Das Funkgespräch hatte die Aufzeichnung in zulässiger Weise gestartet. Da die optische Signalisierung schon beim Beginn des Funkgespräches aktiviert worden war, fiel die Aufzeichnung des Drahtgespräches nicht auf. Der Fehler trat zwar in allen Polizeidirektionen gleichermaßen auf, war aber nur in einer Dienststelle aufgefallen. In dieser Polizeidirektion war dann über den beschriebenen Fehler hinaus durch bewusste Programmierung eine generelle Zwangsaufzeichnung von Nebestellengesprächen herbeigeführt worden.

Ich konnte mich davon überzeugen, dass die Aufzeichnungstechnik nach der Beseitigung des Fehlers ordnungsgemäß arbeitete und den datenschutzrechtlichen Anforderungen entsprach. Die polizeieigenen Test- und Abnahmeprotokolle belegten, dass nunmehr keine unzulässige Zwangsaufzeichnung mehr möglich ist.

Im Ergebnis der Kontrolle habe ich dem Innenminister mitgeteilt, dass in unzulässiger Weise in den Schutzbereich des Artikels 10 Grundgesetz eingegriffen worden war. Ein solcher Eingriff in das Fernmeldegeheimnis wäre nur aufgrund eines Gesetzes gerechtfertigt. Ein Gesetz, das die Aufzeichnung von Telefonaten rechtfertigt, existiert jedoch nicht. Polizeidienstvorschriften, wie die PDV 810 zum Fern-

meldebetriebsdienst oder schriftliche Verfügungen einer Polizeidirektion, genügen diesem Gesetzesvorbehalt nicht.

Die durch gezielte Programmierung herbeigeführte Zwangsaufzeichnung von Gesprächen habe ich gegenüber dem Innenminister beanstandet. Die weitergehende Nutzung derartiger Aufzeichnungen für gerichtliche Verfahren oder Disziplinarverfahren, wie dies in einer Polizeidirektion der Fall war, stellt einen zusätzlichen Eingriff in das Fernmeldegeheimnis dar. Von einer Beanstandung im Zusammenhang mit dem Softwarefehler habe ich abgesehen, da der datenschutzgerechte Zustand sofort hergestellt wurde, nachdem der Fehler festgestellt worden war.

Der Innenminister teilte meine Rechtsauffassung. Um auch künftig unzulässige Änderungen an den Bedientischen und den Dokumentationsanlagen zu verhindern, hat er zusätzlich festgelegt, dass jede Reparatur oder Veränderung durch das Innenministerium genehmigt und anschließend aussagekräftig dokumentiert werden muss. Ich habe darüber hinaus empfohlen, den Umgang mit den Dokumentationssystemen der Polizeidirektionen in Dienstanweisungen zu regeln.

3.3.3 Der anonyme Anruf – ZEVIS-Abrufe nicht immer nachprüfbar

Ein Petent, Halter eines Kraftfahrzeuges, erhielt eines Abends einen anonymen Anruf. Der Anrufer ließ sich zunächst die Halterdaten des Petenten bestätigen. Dann fragte er, ob eine Frau mit dem Fahrzeug zu einem bestimmten Zeitpunkt über einen Autobahnabschnitt in der Nähe von Trier gefahren sei. Dies bestätigte der Petent, da er vermutete, dass der Anrufer einen Zeugen suche. Der Anrufer wollte jedoch lediglich die Telefonnummer der Fahrerin für private Zwecke wissen. Der Petent teilte ihm diese nicht mit. Da er nun eine missbräuchliche Nutzung seiner Daten vermutete, bat er mich um eine datenschutzrechtliche Prüfung.

Im örtlichen und im Zentralen Fahrzeugregister werden neben den Fahrzeugdaten auch die Halterdaten gespeichert. Die Straßenverkehrsbehörde führt das örtliche Register. Das Kraftfahrt-Bundesamt ist für das ins Zentrale Verkehrsinformationssystem (ZEVIS) integrierte Zentrale Fahrzeugregister zuständig. Aus den Registern können unter Beachtung der Vorschriften des Straßenverkehrsgesetzes (StVG) Halterdaten an verschiedene öffentliche Stellen übermittelt und Auskünfte an Private erteilt werden. So darf beispielsweise nach § 39 Abs. 1 StVG Auskunft über den Halter eines Fahrzeuges gegeben werden, wenn der Anfragende unter Angabe des Kennzeichens oder der betreffenden Fahrzeug-Identifizierungsnummer darlegt, dass

er diese Daten zur Verfolgung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr benötigt.

Eine Anfrage bei der zuständigen Straßenverkehrsbehörde ergab, dass dort im fraglichen Zeitraum keine Halterauskünfte zur Person des Petenten erteilt worden sind. Bei der Auswertung der Protokolle des Zentralen Verkehrsinformationssystems beim Kraftfahrt-Bundesamt wurde jedoch festgestellt, dass das Zentrale Verkehrsinformationssystem aus einer Polizeidienststelle unseres Landes wenige Tage vor dem geschilderten Anruf abgefragt worden war. Der Protokollauszug enthielt gemäß § 36 Abs. 6 StVG folgende Angaben: Abfrageterminal, Datum, Uhrzeit, Daten, die für den Suchvorgang eingegeben wurden, sowie das Ergebnis der Recherche. Die bei einem Teil der Abrufe vorgenommene erweiterte Protokollierung nach § 36 Abs. 7 Satz 1 StVG, die sich auch auf den Anlass und die verantwortliche Person erstreckt, war in diesem Fall nicht vorgenommen worden.

Ich habe den Leiter der zuständigen Polizeidienststelle gebeten, mir zum Zwecke der datenschutzrechtlichen Prüfung Anlass und Rechtsgrundlage für den Abruf mitzuteilen. Trotz intensiver Recherche konnte er weder auf der Basis der ZEVIS-Protokolldateien noch mit Hilfe der Identitätsdaten des Betroffenen den konkreten Anlass für die Abfrage und den für den Abruf verantwortlichen Mitarbeiter feststellen. Eine datenschutzrechtliche Prüfung der Angelegenheit war somit nicht möglich. Dieses aus meiner Sicht unbefriedigende Ergebnis musste ich dem Petenten so mitteilen.

Im Rahmen einer Kontrolle bei der Landespolizei habe ich mich auch über die Abrufmöglichkeiten aus ZEVIS informiert (siehe 3.3.1). Dabei hat sich gezeigt, dass es bei der jetzigen Verfahrensweise immer wieder zu solchen Fällen kommen kann, da nicht jede Abfrage umfassend protokolliert wird. Mit INPOL-neu (siehe Vierter Tätigkeitsbericht, Punkt 3.2.1) sollen künftig für jede ZEVIS-Abfrage der Anlass und die für den Abruf verantwortliche Person protokolliert werden, so dass die Rechtmäßigkeit eines Datenabrufes regelmäßig geprüft werden kann.

3.3.4 Polizeiakten im Müllcontainer

Am 27. Juli 2001 wurde ich darüber informiert, dass Unterlagen aus einer Polizeistation in einem Müllcontainer entsorgt worden waren. Ich habe die zuständige Polizeidirektion gebeten, umfassend zu diesem Sachverhalt Stellung zu nehmen.

Der Hausmeister der Polizeistation hatte drei Plastiksäcke mit Altpapier in einem öffentlich zugänglichen Papiercontainer entsorgt. In diesen Säcken befand sich auch

dienstliches Schriftgut, das personenbezogene Daten enthielt, beispielsweise Vorladungen für Beschuldigte, Zeugenanhörungen, Unterlagen aus einer Todesfallermittlung, Fahndungsausschreibungen und eine vertrauliche Mitteilung einer Staatsanwaltschaft.

Der Vorfall wurde in der Polizeidirektion ausgewertet. Im Ergebnis wurde gegen den Hausmeister ein Ermittlungsverfahren wegen des Verdachts der Verletzung von Privatgeheimnissen eingeleitet, und gegen den Leiter der Polizeistation sowie einen weiteren Mitarbeiter wurden disziplinarrechtliche Maßnahmen ergriffen. Darüber hinaus ist das Personal im Zuständigkeitsbereich der Polizeidirektion erneut über den datenschutzgerechten Umgang mit Schriftgut belehrt worden.

Der nicht ordnungsgemäße Umgang mit dem dienstlichen Schriftgut in der betreffenden Polizeistation hat dazu geführt, dass sensible personenbezogene Daten von Bürgern unzulässigerweise Dritten zur Kenntnis gelangen konnten. Ich habe dieses Verhalten gegenüber dem Innenminister beanstandet. Der Minister stimmte mit mir darin überein, dass das Verhalten der Polizeistation einen schwerwiegenden Verstoß gegen datenschutzrechtliche Vorschriften darstellt. Er ging aber davon aus, dass es sich hierbei um einen Einzelfall handelte. Die von der Polizeidirektion getroffenen Maßnahmen lassen hoffen, dass es auch ein einmaliger Vorgang bleibt.

3.3.5 Terrorismusbekämpfungsgesetz

Der Bundestag hat das Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) am 14. Dezember 2001 beschlossen; der Bundesrat hat dem Gesetzespaket am 20. Dezember 2001 zugestimmt. Das umfangreiche Artikelgesetz enthält Änderungen in fast 20 Gesetzen, die zum Teil mit erheblichen Eingriffen in das Recht auf informationelle Selbstbestimmung verbunden sind. So sehr auch verständlich ist, dass nach den Terroranschlägen vom 11. September 2001 in den USA der internationale Terrorismus auch in Deutschland bekämpft werden muss, so geht doch das vorliegende Gesetz sehr weit.

Bundeskriminalamtgesetz

Das Bundeskriminalamt (BKA) kann nunmehr bei sämtlichen öffentlichen und nicht-öffentlichen Stellen ohne nähere Begründung „zur Erfüllung seiner Aufgabe“ als Zentralstelle „oder sonst zu Zwecken der Auswertung“ Daten erheben. Damit wird eine Grauzone eröffnet, die zu Vorfeldermittlungen des BKA ohne justizielle Aufsicht führt. Diese Ermittlungen gehen deutlich über die vom Grundgesetz zugelassene un-

terstützende Zentralstellenfunktion hinaus und ignorieren die Zuständigkeiten der Länder zur Gefahrenabwehr.

Geheimdienstgesetze

Die Verfassungsschutzbehörden, teilweise auch der Militärische Abschirmdienst und der Bundesnachrichtendienst, erhalten umfangreiche Auskunftsbefugnisse gegenüber Luftverkehrsunternehmen, Banken, Post-, Telekommunikations- und Teledienstunternehmen über die dort vorhandenen Daten. Anders als bei polizeilichen Ermittlungen soll es nicht darauf ankommen, ob die Betroffenen sich in irgendeiner Weise strafrechtlich verdächtig gemacht haben. Zwar sollen diese Befugnisse nur über die Behördenleitung beziehungsweise das Ministerium angeordnet werden können, und es sind auch parlamentarische Kontrollen sowie eine spätere Benachrichtigung der Betroffenen vorgesehen. Im Ergebnis jedoch wird durch die neuen Ermittlungsbefugnisse der Geheimdienste auf Gebieten, für die die Polizei zuständig ist, das verfassungsrechtliche Trennungsgebot verletzt.

Pass- und Personalausweisgesetz; Asylverfahrensgesetz, Ausländergesetz

Die Möglichkeit der Aufnahme biometrischer Merkmale in Pässe und Ausweise für deutsche Staatsbürger soll ausdrücklich eröffnet werden. Mit dem Begriff Biometrie oder biometrische Verfahren werden Verfahren zur automatisierten Erfassung und Auswertung personenbezogener Körpermerkmale und personenbezogenen Verhaltens bezeichnet, um Personen automatisiert (wieder)erkennen zu können. Zu den zum gegenwärtigen Zeitpunkt auswertbaren Merkmalen zählen: Fingerabdruck, Handflächenabdruck, Handvenenmuster, Geometrie der Hand, Regenbogen- und Netzhaut des Auges, Gesichtsgeometrie, Stimme, Lippenbewegung, (Unter)Schrift sowie das Tippverhalten auf einer Tastatur.

Vor der Einführung zusätzlicher biometrischer Merkmale ist aus datenschutzrechtlicher Sicht zu prüfen, ob biometrische Verfahren geeignet sind, den weltweit agierenden Terrorismus wirksam zu bekämpfen. Neben der Untersuchung der technischen Aspekte verschiedener Verfahren ist unter anderem zu berücksichtigen, dass deutsche Ausweise mit „Biometrie“ nur dann wirkungsvoll sein können, wenn auch die Ausweise in den anderen Staaten des Schengener Abkommens gleichartig ausgestaltet werden. Bislang lehnen England und Frankreich solche Ausweise jedoch ab. Frankreich hat im „Gesetz bezüglich des rechtlichen Rahmens der Informationstechnologie“ vom Juni 2001 beispielsweise geregelt, dass keine Stelle ohne die ausdrückliche Zustimmung der betroffenen Person verlangen kann, dass diese ihre Identität

anhand eines Verfahrens überprüfen oder bestätigen lässt, welches die Erfassung biometrischer Charakteristiken oder Messungen ermöglicht.

Da für Deutsche zentrale Dateien ausdrücklich ausgeschlossen sind, eignen sich biometrische Merkmale in Ausweisen und Reisepässen ausschließlich zur Überprüfung der Identität von Personen (Verifikation). Nach Aussagen der Bundesdruckerei sind allerdings keine Fälle bekannt, bei denen Personen gefälschte deutsche Ausweise benutzt haben. Die Fälschungssicherheit ist offensichtlich so groß, dass zusätzliche Maßnahmen – zumindest im datenschutzrechtlichen Sinne – nicht unbedingt erforderlich sind. Somit gibt es hinsichtlich der Geeignetheit, Erforderlichkeit und Angemessenheit der Aufnahme zusätzlicher biometrischer Merkmale in Ausweise und Pässe zur Bekämpfung des internationalen Terrorismus einen erheblichen Prüfungsbedarf.

Während bei Deutschen die Einzelheiten einer Aufnahme biometrischer Merkmale in Ausweise und Pässe einem weiteren förmlichen Bundesgesetz vorbehalten bleiben, werden biometrische Merkmale in Dokumenten für Ausländer künftig per Rechtsverordnung durchgesetzt werden. Die Frage, ob diese Merkmale auch außerhalb des Verfügungsbereichs der Betroffenen, also zum Beispiel in zentralen oder dezentralen Referenzdateien, gespeichert werden dürfen, wird für diesen Personenkreis ausdrücklich offen gelassen. Damit sieht das Gesetz die Einführung einer komplexen neuen Technologie vor, ohne offen zu legen, in welchem Rahmen die gespeicherten Merkmale durch die Polizei genutzt werden können. So ist es durch die vorgesehene Speicherung von Sprachprofilen von Ausländern beim BKA und der jetzt schon existierenden zentralen Speicherung von Fingerabdrücken in AFIS (Automatisiertes Fingerabdruck-Identifizierungssystem) nunmehr möglich, eine polizeilich vielfach nutzbare Vorratsdatenverarbeitung aufzubauen. In einer Vielzahl von ausländerrechtlichen Bestimmungen wird ohne Nachweis der Erforderlichkeit und Verhältnismäßigkeit in das Recht auf informationelle Selbstbestimmung der nicht deutschen Bürger eingegriffen. Es ist sogar zu befürchten, dass sensible und für die Betroffenen unter Umständen buchstäblich lebensbedrohliche Informationen aus Asylanträgen ohne Schutzvorkehrungen an Geheimdienste übermittelt werden. So ist selbst die Übermittlung an den Geheimdienst des Verfolgungsstaates nicht mehr ausgeschlossen.

Sicherheitsüberprüfungsgesetz

Durch das vorliegende Gesetz wird der Kreis der Stellen erheblich erweitert, die als sicherheitsempfindlich eingestuft werden, wie lebens- oder verteidigungswichtige Einrichtungen. Damit wird zwangsläufig auch der Kreis der zu überprüfenden Personen ausgedehnt. Die neuen Regelungen sind im Hinblick auf die Terroran-

schläge vom 11. September 2001 grundsätzlich nachvollziehbar und angemessen. Die wesentlichen Festlegungen sollten jedoch im Sicherheitsüberprüfungsgesetz selbst getroffen werden, um ausufernden Überprüfungen im gesamten Versorgungsbereich vorzubeugen. Aus Gründen der Verhältnismäßigkeit erscheint die Einbeziehung des Lebens-/Ehepartners in die Überprüfung zu Zwecken des personellen Sabotageschutzes kritisch.

Zehntes Sozialgesetzbuch

In § 68 SGB X ist nunmehr auch die bisher unzulässige Einbeziehung von Sozialdaten in die Rasterfahndung beschlossen worden. Im Einzelnen dürfen Angaben zur Staats- und Religionszugehörigkeit, frühere Anschriften der Betroffenen, Namen und Anschriften früherer Arbeitgeber sowie Angaben über an Betroffene erbrachte oder demnächst zu erbringende Geldleistungen übermittelt werden, soweit sie zur Durchführung der Rasterfahndung erforderlich sind. Ursprünglich hatte die Bundesregierung geplant, auch die äußerst sensiblen medizinischen Daten in die Rasterfahndung mit einzubeziehen. Fraglich bei dieser gesetzgeberischen Maßnahme ist, warum die bisherige Regelung – die Übermittlung von Sozialdaten an die Polizei im Einzelfall – nicht ausreichte.

3.3.6 Rasterfahndung

Nach den Terroranschlägen vom 11. September 2001 in den USA hat auch der Innenminister unseres Landes die Rasterfahndung gemäß § 44 des Gesetzes über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern (SOG M-V) angeordnet.

Die Rasterfahndung ist eine spezielle Fahndungsmethode, die die Möglichkeiten der elektronischen Datenverarbeitung nutzt. Ihr liegt die Annahme zu Grunde, dass der Verdächtige in automatisiert geführten Dateien einzelne Spuren hinterlassen habe, deren Zusammenführung zu seiner Entlarvung beitragen kann. Deshalb werden vor Beginn einer Rasterfahndung auf der Grundlage einer Fahndungs- oder Ermittlungshypothese Merkmale zusammengestellt, die beim Verdächtigen vorliegen könnten. Die Daten verarbeitenden Stellen, in deren Datensammlungen derartige Merkmale erfasst sind, werden zur Selektion und zur Herausgabe der einschlägigen Datenbestände verpflichtet. Dann werden aus den polizeifremden Datenbeständen die Datenbestände herausgefiltert, auf die eines oder mehrere bestimmte Merkmale zutreffen. Die auf diesem Wege gewonnenen Datensätze werden gegeneinander oder mit zusätzlichen polizeilichen Daten abgeglichen, so dass letztlich eine Restmenge an Daten über möglicherweise

Verdächtige übrig bleibt. Zu diesen Personen werden dann konventionelle Ermittlungen durchgeführt, die den Verdacht ausräumen oder bestätigen sollen.

Auslöser für die Rasterfahndung hier im Lande und in anderen Bundesländern waren Ermittlungen des Bundeskriminalamtes (BKA), die ergaben, dass mindestens drei der mutmaßlichen Attentäter über mehrere Jahre auf dem Gebiet der Bundesrepublik Deutschland wohnhaft gewesen sind. Aufgrund der vorliegenden Erkenntnisse wird angenommen, dass bisher noch nicht identifizierte Mittäter oder Unterstützer, so genannte Schläfer, in der Bundesrepublik wohnhaft sind, als Einzelperson oder als Gruppe für die Begehung weiterer terroristischer Anschläge bereitstehen und diese je nach Lage und Auftrag durchführen würden.

Die Rasterfahndung soll nach den Vorstellungen einer beim BKA eingerichteten Koordinierungsgruppe grob eingeteilt wie folgt ablaufen:

Die Bundesländer erheben aufgrund ihrer Zuständigkeiten zur Gefahrenabwehr die relevanten Daten bei den Einwohnermeldeämtern und den Universitäten/Fachhochschulen. Als Rasterkriterien sind bundesweit vereinbarte Merkmale festgelegt worden. Weiterhin werden Daten aus dem Ausländerzentralregister (AZR) beim Bundesverwaltungsamt vorgerastert. Daten aus diesen drei Bereichen werden zur Vermeidung von Dubletten oder ungeklärten Personenidentitäten einer Qualitätskontrolle unterzogen. Eine Rasterung – wie oben beschrieben – findet in den Bundesländern noch nicht statt. Diese so genannten qualitätsgesicherten Daten werden dann an das Bundeskriminalamt übermittelt. Das BKA stellt diese Daten in eine Verbunddatei ein und hält diese dort vor.

Parallel werden so genannte Abgleichsdateien aus drei Bereichen zusammengestellt:

1. Kernenergie, Gefahrgutlizenzen, Fluglizenzen,
2. Daten (Personaldaten) von privaten Stellen aus dem sicherheitsrelevanten Bereich, um die das BKA auf freiwilliger Basis direkt bittet,
3. Daten aus sonstigen Behörden, Einrichtungen in vorgerasteter Form.

Der Bestand der Verbunddatei wird dann nacheinander mit diesen Datenbeständen abgeglichen.

Bei Übereinstimmung des Datensatzes der Verbunddatei mit dem Datensatz einer Abgleichsdatei (Treffermeldung) erfolgt die Abgabe der Daten an das betreffende

Bundesland. Das Land prüft dann die Personenidentität und stellt weitere konventionelle Recherchen an, wie Abfrage von Prüffällen in Dateien, Recherchen in der Ausländerakte und so weiter. Im Dezember 2001 hatte unser Landeskriminalamt (LKA) die Datensätze so weit aufbereitet, dass sie an das BKA geliefert werden konnten.

Die Rechtslage habe ich sowohl mit dem Innenministerium als auch mit dem LKA erörtert.

Kritikwürdig war aus datenschutzrechtlicher Sicht, dass die erste Anordnung zur Rasterfahndung vom 26. September 2001 nicht darauf hinwies, dass eine Datenübermittlung an das BKA vorgesehen ist. Es entstand somit der Eindruck, dass die Rasterung bis hin zum Datenabgleich mit anderen Dateien im Land selbst stattfindet und gegebenenfalls nur so genannte Treffer an das BKA weitergeleitet werden. Erst die Errichtungsanordnung vom 17. Dezember 2001 stellte klar, dass ein kompletter qualitätsgesicherter Datenbestand an das BKA übermittelt wird.

Rechtlich problematisch bleibt die Datenanlieferung an das BKA trotzdem. Das Bundeskriminalamtgesetz enthält keine Rechtsgrundlage für eine Rasterfahndung durch das BKA. Die Rasterfahndung stellt jedoch eine besondere Maßnahme dar, die gegenüber dem reinen Datenabgleich mit bereits anderweitig speicherungs-fähigen Daten einer ausdrücklichen Rechtsgrundlage im Gesetz bedarf. Das BKA könnte daher in der Phase der Rasterung lediglich eine unterstützende Funktion einnehmen. Insofern spräche eher einiges dafür, dass das BKA die Daten der Länder im Auftrag verarbeitet.

Unzulässig war es, dass das LKA nach der ersten Errichtungsanordnung die Sozialdaten zu Zwecken der Rasterfahndung von den Sozialbehörden angefordert hat und diese auch tatsächlich erhielt. Ich hatte bereits frühzeitig darauf hingewiesen, dass das Sozialgesetzbuch Zehntes Buch (SGB X) eine Einbeziehung von Sozialdaten in die Rasterfahndung nicht erlaubt, da dadurch eine Vielzahl äußerst sensibler Daten von Unverdächtigen ins polizeiliche Visier geraten würde. § 68 SGB X erlaubt eine Datenübermittlung an Polizeibehörden nur im Einzelfall. Das Innenministerium hat inzwischen versichert, dass die unzulässig erhobenen Datenbestände komplett gelöscht worden sind und folglich nicht mehr für einen Datenabgleich genutzt werden.

Rechtlich problematisch ist ebenfalls, dass das BKA umfangreiche Datenbestände von Firmen und Institutionen aus dem sicherheitsrelevanten Bereich auf freiwilliger Basis erbittet, die ebenfalls mit anderen Dateien abgeglichen werden. Es bestehen somit einerseits Datenbestände, die rechtsstaatlich durch eine Anordnung des Innen-

ministers oder durch Richtervorbehalt (je nach Bundesland) abgesichert sind, und andererseits solche Bestände, für die eine derartige Absicherung fehlt. Für Mitarbeiter von Unternehmen, in denen die Unternehmensleitung mit oder ohne Beteiligung des Betriebsrats/Personalrats Personaldaten an das BKA übermittelt hat, bestehen folglich gar keine rechtsstaatlichen Vorkehrungen. Hierzu habe ich das LKA um Stellungnahme gebeten. Die Antwort steht noch aus.

Ein wesentlicher Punkt bei der weiteren Begleitung der Rasterfahndung wird sein, darauf zu achten, dass die nicht mehr benötigten Datenbestände frühzeitig gelöscht werden.

3.3.7 Polizeiliche Datenverarbeitung nicht geheim

Eine Petentin wandte sich mit folgendem Sachverhalt an mich:

Auf dem Weg zu einer Demonstration am Rande einer politischen Veranstaltung im Ausland wurde sie hinter der Grenze von der Polizei festgenommen. Die Maßnahme wurde damit begründet, dass sie Teil einer Gruppe sei, die beabsichtige, die Veranstaltung ernsthaft zu stören. Darüber hinaus ginge von ihrer Person eine besondere Gefahr aus, da sie in Deutschland bereits wegen Körperverletzung verurteilt worden sei. Nach 24 Stunden Abschiebebegewahrsam wurde sie mit einer Sondermaschine nach Deutschland zurückgeflogen. Da die Petentin nicht verurteilt worden war, ersuchte sie die Polizei um Auskunft und bat mich, den Umgang mit ihren personenbezogenen Daten bei der Landespolizei zu prüfen.

Die örtlich zuständige Polizeidirektion hat meine Anfrage und das Ersuchen der Petentin an das Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V) weitergeleitet. Der Direktor des LKA M-V versicherte mir gegenüber mehrfach, dass die Petentin weder in der Polizeilichen Erkenntnisdatei des Landes Mecklenburg-Vorpommern (PED M-V) noch im Informationssystem der Polizei des Bundes und der Länder (INPOL) oder einer weiteren Datenbankanwendung der Landespolizei gespeichert sei. In Absprache mit dem LKA M-V informierte ich die Petentin über dieses Ergebnis.

Den Bundesbeauftragten für den Datenschutz (BfD) bat ich im Wege der Amtshilfe um eine datenschutzrechtliche Prüfung, ob Bundesbehörden Daten der Petentin gespeichert und an die ausländischen Behörden übermittelt hatten.

Der BfD informierte mich darüber, dass – entgegen den bisherigen Mitteilungen des LKA M-V – die Petentin zum Zeitpunkt der Maßnahmen der ausländischen Polizeibehörden im Rahmen des INPOL-Systems noch in einer polizeilichen Datei gespeichert war und das Bundeskriminalamt diese Informationen an die ausländischen Behörden weitergegeben hatte.

Daraufhin habe ich den Direktor des LKA M-V erneut um Stellungnahme gebeten. Zum Redaktionsschluss ergibt sich nunmehr folgendes Bild:

Die Petentin war in einer polizeilichen Datei gespeichert. Grundlage für diese Speicherung war ein Ermittlungsverfahren wegen Körperverletzung, das gegen sie eingeleitet und unter Hinweis auf den Privatklageweg nach § 170 Abs. 2 Strafprozessordnung eingestellt worden war. Die Einstellungsmitteilung wurde von der Staatsanwaltschaft an die örtlich zuständige Polizeidienststelle übersandt, ist seinerzeit aber nicht zum LKA gelangt. Dem Sachverhalt, der dem Strafverfahren zugrunde lag, lässt sich nicht entnehmen, dass es sich hierbei um eine Straftat handelte, die eine Speicherung in der polizeilichen Datei gerechtfertigt hätte. Nachdem das LKA M-V mit mehr als dreijähriger Verspätung vom Verfahrensausgang erfahren hatte, wurden die Daten der Petentin dort umgehend gelöscht. Das LKA M-V verweigert der Petentin gegenüber nach wie vor jede Auskunft über diese Speicherung.

Datenschutzrechtlich sind hierbei folgende Aspekte von Bedeutung:

Falsche/keine Auskunft an die Petentin

Der Petentin wurde über meine Dienststelle durch das LKA M-V eine falsche Auskunft erteilt.

Das LKA M-V verkennt in diesem Zusammenhang, dass jeder in polizeilichen Dateien gespeicherten Person nach den Polizeigesetzen der Länder sowie dem Bundeskriminalamtgesetz grundsätzlich ein Auskunftsanspruch zusteht. Von einer Auskunft kann jedoch abgesehen werden, wenn berechtigte Belange entgegenstehen, so unter anderem eine Gefährdung der Aufgabenerfüllung der Polizei im konkreten Einzelfall. Anhaltspunkte dafür, dass hier ein Fall der zulässigen Auskunftsverweigerung vorlag, lassen sich dem Sachverhalt nicht entnehmen.

Die Verfahrensweise des LKA M-V, der Petentin eine falsche Auskunft zu geben und sie nicht über die zu ihrer Person gespeicherten Daten zu informieren, verstößt gegen die geltenden Bestimmungen zum Auskunftsrecht Betroffener.

Beeinträchtigung schutzwürdiger Belange der Betroffenen

Eine Löschung von Daten hat immer dann zu unterbleiben, wenn schutzwürdige Belange des Betroffenen entgegenstehen. Insbesondere sind Maßnahmen unzulässig, die darauf abzielen oder geeignet sind, den Rechtsschutz von Betroffenen zu vereiteln.

Die in der polizeilichen Datei gespeicherten Daten der Petentin, die das Bundeskriminalamt an die ausländischen Behörden übermittelt hatte, führten zu Beeinträchtigungen ihrer Persönlichkeitsrechte. Das LKA M-V hatte diese Daten eingegeben und war somit verantwortliche Stelle für die Rechtmäßigkeit der Erhebung, die Zulässigkeit der Eingabe sowie die Richtigkeit und Aktualität der Daten. Bis zur endgültigen Klärung des Sachverhaltes sowie bis zum Abschluss der datenschutzrechtlichen Prüfung hätten die Daten wegen des Auskunftsrechts der Petentin, ihres offensichtlichen Interesses an einer Kontrolle der Rechtmäßigkeit der Maßnahme und etwaigen Schadensersatzansprüchen nicht gelöscht werden dürfen.

Obwohl ein Auskunftsersuchen der Petentin vorlag und ich die datenschutzrechtliche Prüfung bereits eingeleitet hatte, wurden die Daten gelöscht. Die schutzwürdigen Belange der Petentin sind dadurch in erheblichem Maße beeinträchtigt und die Wahrnehmung ihrer Rechte erschwert worden.

Zulässigkeit der Speicherung der Daten in der polizeilichen Datei

Die Datei enthält aufgrund ihrer besonderen Zweckbestimmung lediglich Straftaten, die festgelegten Kriterien entsprechen müssen. Dem Sachverhalt lässt sich jedoch nicht entnehmen, dass es sich im vorliegenden Fall um eine solche Straftat handelte.

Es bestehen daher Zweifel, ob die Voraussetzungen für die Aufnahme in diese Datei zum Zeitpunkt der Speicherung vorlagen.

Wahrheitswidrige Mitteilungen an den LfD M-V

§ 27 Abs. 1 DSG MV verpflichtet alle öffentlichen Stellen des Landes, meine Behörde im Rahmen der Aufgabenerfüllung, so auch bei datenschutzrechtlichen Prüfungen, in jeder Hinsicht zu unterstützen und dabei insbesondere umfassend Auskünfte zu geben, Unterlagen vorzulegen und Einsicht in Dateien zu gewähren. Nur so wird eine im Sinne der Artikel 6 und 37 der Verfassung des Landes Mecklenburg-Vor-

pommern ordnungsgemäße und unabhängige Prüfung der Wahrung des Grundrechtes auf informationelle Selbstbestimmung der Betroffenen gewährleistet.

Das LKA M-V hat meine Anfrage nicht wahrheitsgemäß beantwortet, die Unterlagen vernichtet und die Daten gelöscht. Mit dieser Verfahrensweise hat es seine Mitwirkungspflichten in erheblichem Maße verletzt und die datenschutzrechtliche Kontrolle in unzulässiger Weise behindert.

Diese Verstöße gegen das geltende Datenschutzrecht werde ich gegenüber dem Innenminister unseres Landes gemäß § 28 Abs. 1 Satz 1 Nr. 1 DSGVO beanstanden und Maßnahmen empfehlen, um künftig eine datenschutzgerechte Verfahrensweise zu gewährleisten. Insbesondere sollten die Umstände dieses Einzelfalles aufgeklärt und die Petentin umfassend informiert werden.

3.4 Verkehr

3.4.1 Rund ums Knöllchen – Datenverarbeitung in Bußgeldstellen

Nicht immer gelangen Schreiben der Verwaltung an den richtigen Adressaten. Das musste auch ein Petent erfahren, der einen an ihn gerichteten Bescheid erst auf Umwegen erhielt. In der Anschrift fehlte die Hausnummer, und so bekam eine andere Person gleichen Namens in derselben Straße seine Post und konnte die für den Petenten bestimmten Daten zur Kenntnis nehmen. Der Petent hat mich gebeten, diesen Sachverhalt zu prüfen.

Der vom Kraftfahrt-Bundesamt im automatisierten Verfahren übermittelte Datensatz für Straßennamen und Hausnummer wurde nur unvollständig übernommen, weil das vorhandene Verfahren nur eine Datensatzlänge von 25 Zeichen zuließ. Längere Datensätze werden in einer gesonderten Liste ausgewiesen und müssen manuell ergänzt werden. Dabei war in diesem Einzelfall offensichtlich ein Fehler aufgetreten. Ich habe die Bußgeldstelle auf den Fehler aufmerksam gemacht, woraufhin sie das Verfahren modifizierte. Die Fehlerlisten werden nunmehr für die einzelnen Bearbeiter gesondert ausgedruckt. Jetzt kann jeder Bearbeiter seine Vorgänge vollständig bis zum Postausgang in eigener Verantwortung erledigen. Ich habe ergänzend empfohlen, dies in den Listen entsprechend zu dokumentieren. Des Weiteren sollte mittelfristig auch die Software geändert werden, so dass eine vollständige Übernahme aller Datensätze im automatisierten Verfahren möglich ist. Dadurch würde zum einen diese Fehlerquelle beseitigt und zum anderen würden aufwendige Nacharbeiten entfallen.

In einem anderen Fall erhielt ein Petent gleich zwei Verwarnungsgeldangebote, wobei nur eines für ihn bestimmt war. In der Bußgeldstelle war beim Kuvertieren der Bescheide ein Fehler aufgetreten. Die Kuvertiermaschine wird über einen Strichcode gesteuert. Dieser Code ist auf den Bescheiden aufgedruckt und wird von der Maschine gelesen. Weiterhin verfügt die Kuvertiermaschine über eine Doppelblattkontrolle. Bei Fehlern hält die Maschine an, und der Bediener muss den unverschlossenen Briefumschlag dem Auffangkorb entnehmen und prüfen. Darüber hinaus kontrollieren die Bearbeiter nach dem Kuvertieren nochmals, ob die Adresse im Brieffenster zu erkennen ist, der Brief verschlossen ist und keine sonstigen Auffälligkeiten aufweist. Bei dieser Arbeitsweise dürfte ein derartiger Fehler nicht unentdeckt bleiben. Wie es in dem konkreten Fall dennoch dazu kam, war nicht mehr aufzuklären. Nach Mitteilung der Bußgeldstelle ist ein Fehler der Mitarbeiter aufgrund der an diesem Tag ca. 1.600 unter Zeitdruck zu kuvertie-

renden Bescheide jedoch nicht auszuschließen. Dieser Tatsache geschuldet konnten offensichtlich die durch die Kuvertiermaschine angezeigten Fehler nicht ordnungsgemäß überprüft werden. Auch für eine abschließende Kontrolle der kuvertierten Bescheide fehlte die Zeit. Die Mitarbeiter der Bußgeldstelle wurden nochmals über die ordnungsgemäße Überwachung der Kuvertiermaschine belehrt. Darüber hinaus soll sichergestellt werden, dass den Mitarbeitern für das Kuvertieren und die anschließende Kontrolle genügend Zeit bleibt, um solche Verstöße künftig auszuschließen.

Insgesamt zeigt sich, dass auch der zunehmende Einsatz von Technik Risiken für den Datenschutz in sich birgt und deshalb ergänzende technische und organisatorische Maßnahmen erforderlich sind.

Bei Kontrollen in einzelnen Bußgeldstellen des Landes habe ich vor allem folgende Mängel festgestellt und Empfehlungen gegeben, wie diese zu beheben sind:

- Dateibeschreibungen gemäß § 16 Landesdatenschutzgesetz von Mecklenburg-Vorpommern (DSG MV) lagen teilweise nicht oder nur unvollständig vor. Sie waren durch die Bußgeldstellen zu fertigen beziehungsweise zu ergänzen.
- In einigen Bußgeldstellen wurden noch zu viele Daten erhoben (siehe Dritter Tätigkeitsbericht, Punkt 3.3.2). Die entsprechenden Vordrucke sind inzwischen geändert worden. Auf die regelmäßige Erhebung der Angabe "Beruf" und "Nationalität" konnte mangels Erforderlichkeit der Daten verzichtet werden. Auf den Erhebungsvordrucken waren in einzelnen Fällen die datenschutzrechtlichen Hinweise zur Aufklärung des Betroffenen zu ergänzen.
- In einigen Fällen wurden Datenträger nicht ordnungsgemäß aufbewahrt, und es fehlten technische Maßnahmen zur sicheren Unterbringung von Servern.
- Mitunter wurden die Aufbewahrungs- und Speicherfristen nicht beachtet. Die Akten wurden erst nach Löschung der Daten im automatisierten Verfahren ausgesondert. Da in manchen Fällen bisher noch kein oder nur einmal jährlich ein Auslagerungslauf stattfand, wurden die Aufbewahrungsfristen für Akten nach der Richtlinie des Wirtschaftsministeriums vom 3. März 1999 bei weitem überschritten. Die nunmehr in regelmäßigen Abständen, meist vierteljährlich, stattfindenden Auslagerungsläufe und die damit verbundene Aussonderung von Akten trägt zu einer fristgerechten Löschung der Daten bei.

Insgesamt war die Zusammenarbeit mit allen beteiligten Stellen konstruktiv, so dass die datenschutzrechtlichen Bedingungen bei der Verarbeitung personenbezogener Daten in Ordnungswidrigkeitenverfahren wesentlich verbessert werden konnten.

3.4.2 Videoaufzeichnungen im Rahmen der Verkehrsüberwachung

Petenten beschwerten sich bei mir, dass das Ordnungsamt einer Stadt heimlich Videoaufzeichnungen anfertige, um sie dann als Beweismittel in Ordnungswidrigkeitenverfahren zu nutzen. Es sei nicht erkennbar, ob lediglich einzelne Verkehrsverstöße erfasst oder sämtliche Verkehrsteilnehmer aufgezeichnet würden, so dass sich die Frage der Zulässigkeit dieser Verfahrensweise stelle.

Meine Prüfung hat ergeben, dass mit der Videokamera vor allem Verstöße gegen die Gurtanlagepflicht, die Beachtung des Rotlichtes sowie des Grünpfeils an Ampeln dokumentiert werden. Zur Überwachung von Verkehrsteilnehmern, die das Rotlicht sowie das Haltegebot am Grünpfeil missachten, kommen Videokameras vor und hinter der Ampel zum Einsatz. Während die Kamera hinter der Ampel lediglich gezielt bei einem festgestellten Verstoß eingeschaltet wird, zeichnet die Kamera vor der Ampel das gesamte Verkehrsgeschehen ununterbrochen auf. Die Einstellung dieser Kamera führt dazu, dass hiervon auch Fahrzeugführer, Insassen und Fußgänger erfasst werden, die sich ordnungsgemäß verhalten. Begründet wird die dauerhafte Aufzeichnung damit, dass es bei der Verwertung des Beweismittels nicht allein auf das Überfahren der Haltlinie bei Rot, sondern auch auf die Dauer der Gelbphase ankomme.

Bei der Verfolgung von Verstößen gegen die Gurtanlagepflicht durch zwei Verkehrsüberwacher kontrolliert der erste Mitarbeiter, welcher Fahrzeugführer nicht angeschnallt ist, und teilt dies dem zweiten Mitarbeiter über Funk mit, der daraufhin den Verstoß mit der Videokamera aufzeichnet. Nimmt lediglich ein Verkehrsüberwacher diese Aufgabe wahr, richtet er die Videokamera auf die entgegenkommenden Fahrzeuge, prüft durch den Sucher, ob der jeweilige Fahrzeugführer einen Sicherheitsgurt angelegt hat, und zeichnet Verstöße auf. Bei dieser Vorgehensweise führen jedoch verschiedene Faktoren, wie Tageslicht, Witterung, getönte Scheiben des Fahrzeugs, dunkle Kleidung und Entfernung, dazu, dass der einzelne Verkehrsüberwacher häufig nicht oder nicht rechtzeitig erkennen kann, ob der Fahrzeugführer den Sicherheitsgurt tatsächlich angelegt hat. Im Ergebnis waren so auf einer von mir geprüften Videosequenz von den aufgezeichneten Fahrzeugführern nur wenige dabei, die keinen Haltegurt angelegt hatten. Die meisten Personen verhielten sich ordnungsgemäß.

Die Mitarbeiter im Ordnungsamt überprüfen die Aufzeichnungen und überspielen die Vorgänge, die eine Ordnungswidrigkeit beinhalten, auf eine Videokassette. Zusätzlich wird ein Ausdruck erstellt und zur jeweiligen Akte genommen. Das Ordnungsamt nutzt die Kamerakassette innerhalb weniger Tage für neue Aufzeichnungen, so dass alle für Ordnungswidrigkeitenverfahren nicht relevanten Vorgänge durch Überspielen gelöscht werden.

Gegen die vom Ordnungsamt gewählte Verfahrensweise habe ich Bedenken geäußert, weil viele Personen erfasst werden, die keine Ordnungswidrigkeit begangen haben. Ferner fehlen normenklare gesetzliche Regelungen zum Einsatz von Videotechnik im Rahmen der Verkehrsüberwachung. Im Ergebnis hat die Stadt die Verfahrensweise modifiziert. Künftig werden Kontrollen der Gurtanlegepflicht grundsätzlich durch zwei Mitarbeiter durchgeführt, so dass tatsächlich nur bei einem Anfangsverdacht einer Ordnungswidrigkeit aufgezeichnet wird. Darüber hinaus wird nunmehr zur Überwachung von Verstößen gegen das Rotlicht an Ampeln die Kamera vor der Ampel erst kurz vor Beginn der Gelbphase eingeschaltet, um somit die Aufzeichnung der sich ordnungsgemäß verhaltenden Verkehrsteilnehmer auf ein Minimum zu reduzieren.

Das Wirtschaftsministerium unseres Landes sieht ebenfalls Regelungsbedarf. Es hat mir den Entwurf eines Erlasses über die Anfertigung und die Verwendung von Video- und sonstigen Bildaufzeichnungen als Beweismittel bei der Verkehrsüberwachung durch Kommunen (Beweisbild-Erlass) zur Stellungnahme übersandt. Der Erlass knüpft an die allgemeinen Befugnisnormen zur Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten gemäß §§ 24, 24a Straßenverkehrsgesetz an und geht davon aus, dass Bildaufzeichnungen grundsätzlich nur beim Anfangsverdacht einer Ordnungswidrigkeit angefertigt werden. Darüber hinaus enthält er jedoch auch sehr weitgehende Ausnahmen. Ich habe in meiner Stellungnahme auf Folgendes hingewiesen:

Das Straßenverkehrsgesetz enthält keine Vorschrift für personenbezogene Videoaufzeichnungen im Rahmen der Verkehrsüberwachung. § 46 Ordnungswidrigkeitengesetz in Verbindung mit § 100c Abs. 1 Nr. 1a Strafprozessordnung lässt zwar das Herstellen von Lichtbildern und Aufzeichnungen ohne Wissen des Betroffenen zu. Hierfür muss jedoch ein Tatverdacht gegen den Betroffenen vorliegen. Für Videoaufzeichnungen zur Verkehrsüberwachung sollte daher eine normenklare Rechtsgrundlage geschaffen werden, mit der unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit ein verbindlicher Rahmen für Eingriffe in das Grundrecht auf informationelle Selbstbestimmung festgelegt wird.

Ferner sind die im Erlass vorgesehenen Ausnahmen zu weit gefasst. Diese könnten in der Praxis dazu führen, dass im Rahmen der Verkehrsüberwachung zunächst sehr umfangreich aufgezeichnet wird, um anschließend die beweisrelevanten Mitschnitte zu gewinnen. Eine solche Verfahrensweise ist jedoch datenschutzrechtlich bedenklich. Die Überwachung bestimmter Verkehrsordnungswidrigkeiten, bei denen Bildaufzeichnungen als Beweismittel notwendig sein können, ist bereits in verschiedenen Erlassen geregelt. Im Hinblick auf die nunmehr vorgesehenen Ausnahmen würden die in diesen Erlassen normierten Anforderungen unterlaufen. Deshalb sollten die Ausnahmen enger gefasst und dabei auch die bereits in anderen Erlassen aufgestellten Kriterien berücksichtigt werden.

Das Wirtschaftsministerium beabsichtigt, den Erlass zu überarbeiten und mir Anfang des Jahres 2002 einen neuen Entwurf vorzulegen.

3.4.3 Straßenbenutzungsgebühren

In meinem Zweiten Tätigkeitsbericht hatte ich unter Punkt 2.19.1 über die Pläne der Bundesregierung berichtet, Autobahnbenutzungsgebühren (Maut) automatisch zu erfassen. Bereits 1995 wurde ein Feldversuch mit automatischen Gebührenerfassungssystemen durchgeführt.

Im Sommer 2001 wurden erneut Pläne der Bundesregierung bekannt, Straßenbenutzungsgebühren zu erheben. Das Bundeskabinett hatte am 15. August 2001 den Gesetzentwurf für die Einführung eines Mautsystems für Lastkraftwagen beschlossen (Autobahnmautgesetz für schwere Nutzfahrzeuge – ABMG). Es ist vorgesehen, ab 2003 neben der manuellen Erfassung der Gebühren ein automatisches System einzuführen, mit dem eine streckenbezogene Autobahnbenutzungsgebühr für Lastkraftwagen erhoben werden soll. Für das automatische System sollen das Satellitennavigationssystem GPS und die Mobilfunktechnologie genutzt werden. Dadurch werden stationäre Erfassungseinrichtungen entbehrlich. Relativ einfach könnte so das mautpflichtige Straßennetz beispielsweise auf den Bereich der Bundesstraßen ausgedehnt werden. Selbst ein grenzüberschreitender Einsatz derartiger Systeme wäre aus technischer Sicht leicht zu realisieren.

Das Projekt ist datenschutzrechtlich relevant, weil die vorgesehene Technik es prinzipiell ermöglicht, den Fahrweg der Mautpflichtigen detailliert zu dokumentieren und zu archivieren und auf diese Weise exakte Bewegungsprofile zu erstellen. Damit kön-

nen Systembetreiber und andere nachvollziehen, wer wann wohin wie lange gefahren ist.

In einer Entschließung vom 1. Oktober 2001 (siehe Anlage 20) haben die Datenschutzbeauftragten des Bundes und der Länder darauf hingewiesen, dass elektronische Mautsysteme datenschutzgerecht ausgestaltet werden müssen. Bei der Gestaltung und dem Betrieb der erforderlichen Erfassungs- und Kontrollsysteme soll darauf geachtet werden, dass das im Bundesdatenschutzgesetz normierte Prinzip der Datensparsamkeit sichergestellt wird. Insofern sind Verfahren prädestiniert, bei denen Mautgebühren vorab entrichtet werden können und somit keine personenbeziehbaren Daten erhoben und gespeichert werden müssen. In der Entschließung wurde zudem deutlich gemacht, dass die bereits 1995 formulierten Anforderungen nach wie vor aktuell sind. So darf auch bei den jetzt geplanten Systemen die Überwachung der Gebührenerhebung nur stichprobenweise erfolgen und die Identität der Mautpflichtigen nur dann aufgedeckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Gebühren nicht ordnungsgemäß entrichtet worden sind. Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Mautpflichtigen durchschaubar sein. Sie müssen sich jederzeit über den Abrechnungsvorgang informieren sowie den eventuellen Kontrollvorgang erkennen können. Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, dass sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können. Es ist sicherzustellen, dass anfallende personenbezogene Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen.

Anfang Oktober 2001 lag auch ein Gesetzentwurf vor, nach dem Mautgebühren für die Kraftfahrzeuge erhoben werden dürfen, die privat finanzierte Brücken, Tunnel, Gebirgspässe oder mehrspurige Bundesstraßen mit getrennten Fahrbahnen benutzen.

Die Datenschutzbeauftragten gingen in der oben genannten Entschließung auch auf diesen Entwurf ein und forderten, dass an der dort vorgesehenen Barzahlungsmöglichkeit ohne Verarbeitung personenbezogener Daten unbedingt festgehalten werden muss, da nur diese Zahlungsweise die weitergehende Datenerfassung für alle Mautpflichtigen (Kennzeichen und Bilder der Fahrzeuge) vermeidet.

Es ist zu erwarten, dass die zum Einsatz kommenden Erfassungssysteme mit einem Minimum an personenbezogenen Daten auskommen und somit den Anforderungen der Datensparsamkeit genügen werden.

3.5 Verfassungsschutz

3.5.1 Novellierung des Landesverfassungsschutzgesetzes

Am 11. Juli 2001 ist das novellierte Landesverfassungsschutzgesetz Mecklenburg-Vorpommern (LverfSchG M-V) in Kraft getreten. Bereits im Laufe des Gesetzgebungsverfahrens habe ich zu datenschutzrechtlich relevanten Aspekten des Entwurfes beraten.

Neu ist, dass

- dem Bürger nunmehr Auskunft zu erteilen ist, ohne dass er ein besonderes Interesse darlegen muss. Auch zur Herkunft der Daten und zu Übermittlungen ist der Bürger nun grundsätzlich zu informieren. Der Gesetzgeber ist damit einer alten Forderung der Datenschutzbeauftragten (siehe auch Zweiter Tätigkeitsbericht, Punkt 2.5.3) nachgekommen. Mit diesen erweiterten Auskunftspflichten der Verfassungsschutzbehörde wurde das Recht des Bürgers auf informationelle Selbstbestimmung gestärkt.
- Daten bei unerledigten Auskunftsanträgen nicht gelöscht werden dürfen. Dies dient dem Rechtsschutz der Betroffenen und ist daher auch aus datenschutzrechtlicher Sicht positiv zu werten.
- der Verfassungsschutz nunmehr auch Bestrebungen beobachten darf, „die gegen den Gedanken der Völkerverständigung oder gegen das friedliche Zusammenleben der Völker gerichtet sind“. In der Gesetzesbegründung wird dargelegt, dass hierdurch vornehmlich Aktivitäten des rechtsextremistischen Spektrums erfasst werden sollen, die zum Beispiel eine Revision der Grenzen zu östlichen Nachbarländern Deutschlands fordern und hierbei jene Nationen als ethnisch „minderwertig“ darstellen. Eingriffsbefugnisse des Staates verlangen nach einer gesetzlichen Grundlage. Die Ausführungen in der Gesetzesbegründung sind dafür nicht ausreichend.
- Daten bei Dritten nunmehr unter den gleichen Voraussetzungen wie bei der betroffenen Person selbst – ohne deren Kenntnis – erhoben werden dürfen. Eine inhaltliche Begründung, warum keine Abstufung mehr bei den Voraussetzungen erfolgt, wird nicht gegeben. Derart weitreichende Befugnisse für eine Datenerhebung bei Dritten sind aus anderen Landesverfassungsschutzgesetzen nicht bekannt. Ebenso wenig ist im Bundesverfassungsschutzgesetz in dieser konkreten Form eine Datenerhebung bei Dritten angesprochen.

- die nachrichtendienstlichen Mittel zur heimlichen Informationsbeschaffung im Gesetz selbst abschließend aufgezählt sind. Unter dem Aspekt der Normenklarheit ist das positiv zu werten. Allerdings hätte in der Gesetzesbegründung erläutert werden sollen, was unter den einzelnen nachrichtendienstlichen Mitteln zu verstehen ist. Die Datenerhebung mit derartigen Mitteln stellt einen tiefen Eingriff in das Recht auf informationelle Selbstbestimmung dar und verlangt daher nach einer Erklärung. Ferner sind die Voraussetzungen, unter denen nachrichtendienstliche Mittel auch bei Dritten eingesetzt werden können, aus datenschutzrechtlicher Sicht sehr weit gefasst.
- über das heimliche Mithören und Aufzeichnen des nicht öffentlich gesprochenen Wortes unter Einsatz technischer Mittel außerhalb von Wohnungen die betroffene Person nunmehr nachträglich informiert werden soll. Allerdings wurde nicht für alle verdeckten Maßnahmen eine solche Mitteilungspflicht in das Gesetz aufgenommen, obwohl hierzu eine entsprechende Empfehlung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 vorlag (siehe Anlage 1). Ich hatte darauf hingewiesen, dass ein Betroffener nur dann von den ihm zustehenden Rechten nach Art. 19 Abs. 5 Grundgesetz (Rechtsschutzgarantie) Gebrauch machen kann, wenn er auch weiß, dass nachrichtendienstliche Mittel eingesetzt worden sind.

3.6 Einwohnerwesen

3.6.1 Melderechtsrahmengesetz

Mit einer umfassenden Änderung des Melderechtsrahmengesetzes sollen für das melderechtliche Verfahren die Möglichkeiten der modernen Informations- und Kommunikationstechnologie genutzt und somit die Voraussetzungen für die Gestaltung zukunftsorientierter Verwaltungsabläufe geschaffen werden. Zu einem Referentenentwurf des Bundesministerium des Innern habe ich gegenüber unserem Innenministerium Stellung genommen und datenschutzrechtliche Empfehlungen gegeben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich ebenfalls sehr frühzeitig an der Diskussion beteiligt und auf ihrer Sitzung am 8./9. März 2001 eine EntschlieÙung zur Novellierung des Melderechtsrahmengesetzes verabschiedet (siehe Anlage 17). Die Datenschutzbeauftragten haben dabei auf Folgendes hingewiesen:

- Der Entwurf enthält datenschutzrechtlich bedenkliche Tendenzen zur Zentralisierung von Melderegistern.
- Einfache Melderegisterauskünfte über das Internet verhindern eine hinreichende Prüfung der schutzwürdigen Belange der Betroffenen. Eine solche Verfahrensweise sollte daher auf die Einwilligung der Betroffenen gestützt werden. Zumindest sollte ihnen ein Widerspruchsrecht gegen diese Auskunftsform eingeräumt werden.
- Um die schutzwürdigen Interessen der Betroffenen bei elektronischen Abrufverfahren über das Internet zu wahren, sollte auch bei öffentlichen Stellen die fortgeschrittene elektronische Signatur nach dem Signaturgesetz eingesetzt werden (siehe auch Punkt 3.17.2).
- Die Auskunftssperre bei Gefahren für Leib und Leben oder ähnlich hochrangige Rechtsgüter muss bei Melderegisterauskünften uneingeschränkt gelten. Erteilt die Meldebehörde im Einzelfall dennoch auf der Basis einer Risikoabwägung ohne Einwilligung des Betroffenen eine Auskunft, so könnte ihn dies erheblich gefährden.
- Die Widerspruchslösung, die bisher bei Datenübermittlungen an Parteien und Wählergruppen im Vorfeld von Wahlen für Wahlwerbezwecke vorgesehen ist, hat sich in der Praxis als weitgehend unwirksam erwiesen. Daher sollte sie durch eine Einwilligungsregelung ersetzt werden.

- Die Hotelmeldepflicht und die damit verbundene millionenfache Datenerhebung sollte mangels Erforderlichkeit abgeschafft werden.

Der mittlerweile vorgelegte Gesetzentwurf der Bundesregierung zur Änderung des Melderechtsrahmengesetzes und anderer Gesetze vom 17. August 2001 (BR-Drs. 578/01) hat diese Hinweise kaum berücksichtigt. Positiv hervorzuheben ist lediglich, dass dem Betroffenen bei Melderegisterrückkünften über das Internet zumindest ein Widerspruchsrecht eingeräumt worden ist. Darüber hinaus wurde von der ursprünglichen Absicht Abstand genommen, Melderegister mehrerer Meldebehörden gemeinsam zu nutzen.

Es bleibt zu hoffen, dass die Anregungen und Hinweise der Datenschutzbeauftragten im weiteren Gesetzgebungsverfahren noch Berücksichtigung finden, um so zu einem angemessenen Interessenausgleich zu gelangen.

3.6.2 Probleme mit dem Widerspruchsrecht bei Meldebehörden

Über die Möglichkeiten der Bürger, bei den Meldebehörden gegen die Weitergabe ihrer Daten zu widersprechen, habe ich in der Vergangenheit mehrfach berichtet (siehe Erster Tätigkeitsbericht, Punkt 2.3.5 und Vierter Tätigkeitsbericht, Punkt 3.4.3). Dieses Recht der Betroffenen, gegen die Weitergabe ihrer Daten an

- Parteien, Wählergruppen und andere Träger von Wahlvorschlägen zum Zwecke der Wahlwerbung gemäß § 35 Abs. 1 Landesmeldegesetz (LMG),
- Mandatsträger, Presse oder Rundfunk zum Zwecke der Ehrung bei Alters- oder Ehejubiläen nach § 35 Abs. 2 LMG,
- Adressbuchverlage zur Herausgabe eines Einwohneradressbuches gemäß § 35 Abs. 3 LMG sowie
- Religionsgesellschaften ihrer Angehörigen, der sie selber nicht angehören, gemäß § 32 Abs. 2 LMG

zu widersprechen, ist zu einem Dauerthema geworden. Besonders vor Wahlen und vor der Herausgabe von Adressbüchern wenden sich nach wie vor viele Bürger an mich, deren Meldedaten ohne ihre Zustimmung übermittelt wurden. Mir bleibt in diesen Fällen nichts anderes übrig, als auf die gesetzliche Regelung zu verweisen, wo-

nach statt einer Einwilligung der Betroffenen lediglich ein Widerspruchsrecht vorgesehen ist.

Die für den Bürger oft nur schwer durchschaubaren Regelungen sollten zumindest in den Meldebehörden des Landes hinreichend bekannt sein, damit eine datenschutzgerechte Umsetzung gewährleistet werden kann. Das Innenministerium als oberste Fachaufsichtsbehörde hat die Meldebehörden in den vergangenen Jahren mehrfach auf die Rechtslage hingewiesen. Dennoch war im Berichtszeitraum erneut festzustellen, dass in der Praxis gegen die melderechtlichen Bestimmungen verstoßen wurde.

So hatte eine Stadt ihre Einwohner im amtlichen Bekanntmachungsblatt über die geplante Datenweitergabe an einen Adressbuchverlag sowie die Möglichkeit des Widerspruchs ordnungsgemäß informiert. Es wurde ein Termin genannt, bis zu dem der Widerspruch erhoben werden konnte. Die Daten wurden einen Monat nach diesem Stichtag an den Verlag übermittelt. Dabei sind aber auch die Daten von Einwohnern übermittelt worden, die erst nach dem Stichtag zugezogen waren. Zwar wird bei der Anmeldung im Anmeldeformular auf die Widerspruchsrechte hingewiesen, jedoch war beispielsweise ein Petent aufgrund der Veröffentlichung davon ausgegangen, dass die Frist hierfür bereits abgelaufen sei. Einen gesonderten Hinweis zum geplanten Adressbuch gab es für die neuen Einwohner nicht. Diese unklare Verfahrensweise führte zu Beschwerden. Ich habe dem Bürgermeister Hinweise zu einer datenschutzgerechten Umsetzung gegeben und empfohlen, das Verfahren für die Betroffenen transparenter zu gestalten. Der Bürgermeister wird meine Hinweise künftig berücksichtigen. Aufgrund der Proteste von Einwohnern will die Einwohnermeldebehörde jedoch in absehbarer Zeit keine Daten mehr an Adressbuchverlage übermitteln.

In einem anderen Fall hatte der Vorsteher eines Amtes in den vergangenen Jahren versäumt, die Einwohner regelmäßig über ihre Widerspruchsrechte zu unterrichten. Meinen Hinweis auf die Bekanntmachungspflicht nach § 36 LMG nahm er zum Anlass, in der Tageszeitung in sehr kurzer Form über die gesetzlichen Vorschriften zu informieren, ohne jedoch mitzuteilen, welche Datenübermittlungen dies im Einzelnen betrifft. Da das Amt über kein eigenes Mitteilungsblatt verfügt, sollte die Veröffentlichung so knapp wie möglich gehalten werden, um Kosten zu sparen. Ich habe ihn darauf hingewiesen, dass in diesem Fall die mit § 36 LMG verbundene Aufklärung der Betroffenen keinesfalls erreicht wurde. Nach einer intensiven Diskussion wurde in der örtlichen Presse nochmals ein etwas erweiterter und modifizierter Hinweis nach § 36 LMG veröffentlicht und auch auf die Schaukästen der einzelnen Gemeinden verwiesen, in denen ausführliche Informationen zum Widerspruchsrecht ausgehängt wur-

den. Das Ergebnis ist aus datenschutzrechtlicher Sicht zufriedenstellend. Der Fall macht deutlich, wie vielfältig die Gründe dafür sein können, dass dem Betroffenen die Wahrnehmung seines Rechtes auf informationelle Selbstbestimmung erschwert wird.

In einem weiteren Fall hatte die Meldebehörde im Rahmen der jährlichen Bekanntmachungspflicht nach § 36 LMG die Einwohner zwar auf die Widerspruchsrechte hingewiesen, aber die Möglichkeit des Widerspruches nur für einen Zeitraum von vier Wochen eingeräumt. Tatsächlich ist die Wahrnehmung dieses Rechtes jedoch an keine Fristen gebunden. Obwohl die Meldebehörde zugesagt hatte, dies künftig zu beachten, trat bei der erneuten Bekanntmachung wieder derselbe Fehler auf. Ich habe empfohlen, nunmehr eine Veröffentlichung vorzunehmen, die den melderechtlichen Vorschriften entspricht. Eine Antwort steht noch aus.

Es ist zu befürchten, dass auch künftig derartige Fehler zu Lasten der Betroffenen gehen. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder empfohlen, das Widerspruchsrecht durch die bürgerfreundlichere Einwilligung zu ersetzen (siehe auch Punkt 3.6.1).

3.7 Kommunales

3.7.1 Zweckbindung von Daten gilt auch für Gemeindevertreter

Ein Petent hatte dem Gemeindevorstand mitgeteilt, dass ein Mitglied der Stadtvertretung die Voraussetzungen der Wählbarkeit nicht erfülle, da – entgegen der Eintragung im Melderegister – er in der Gemeinde lediglich den Nebenwohnsitz habe. Der Vorsitzende der Stadtvertretung hörte den Stadtvertreter hierzu an und übersandte ihm zu diesem Zweck eine Kopie des Schreibens des Petenten. Ein Jahr später wurde dieses Schreiben in einem Arbeitsgerichtsprozess verwendet, an dem weder der Petent noch die Stadt beteiligt waren. Im Rahmen meiner Prüfung habe ich festgestellt, dass der Stadtvertreter den Brief des Petenten nach seinem Ausscheiden aus der Stadtvertretung an eine der Prozessparteien weitergereicht hatte. Ich habe den Umgang mit den personenbezogenen Daten in diesem Fall nach § 28 Abs. 1 Landesdatenschutzgesetz von Mecklenburg-Vorpommern (DSG MV) beanstandet und den Vorgang wie folgt bewertet:

Die Verantwortung für den rechtmäßigen Umgang mit personenbezogenen Daten in den kommunalen Vertretungskörperschaften obliegt dem verwaltungsleitenden Organ der Kommune, dem Vorsitzenden der Gemeindevertretung und den Mitgliedern der Gemeindevertretung gleichermaßen.

Die Nutzung personenbezogener Daten steht nach § 9 Abs. 1 DSG MV unter dem Vorbehalt der Erforderlichkeit. Erforderlich ist eine Nutzung für den angestrebten Zweck nur dann, wenn keine anderen geeigneten Mittel vorhanden sind, die die Rechte des Betroffenen weniger beeinträchtigen. In diesem Fall war die Weitergabe des Schreibens durch den Vorsitzenden der Stadtvertretung zum Zwecke der Anhörung des Stadtvertreters nicht erforderlich, da die im Schreiben genannten Einzelheiten für die Frage, ob dieser seinen Hauptwohnsitz im Wahlgebiet hat, nicht relevant waren. Es wäre im Rahmen der Anhörung ausreichend gewesen, auf das Schreiben in allgemeiner Form hinzuweisen.

Nach § 10 DSG MV ist das Verarbeiten personenbezogener Daten zulässig, wenn es zur rechtmäßigen Aufgabenerfüllung erforderlich ist. Das Schreiben des Petenten wurde dem Stadtvertreter lediglich zur Stellungnahme hinsichtlich seines Hauptwohnsitzes übergeben, um die Rechtmäßigkeit seiner Mitgliedschaft in der Vertretungskörperschaft zu prüfen. Ausschließlich in diesem Zusammenhang war er befugt, mit den Daten umzugehen. Für die Weitergabe des Schreibens an eine der Prozessparteien gab es keine Rechtsgrundlage, so dass die Datenübermittlung unzulässig war. Nach dem Ausscheiden aus der Stadtvertretung wäre er verpflichtet

gewesen, das Schreiben entweder an den Vorsitzenden der Stadtvertretung zurückzugeben oder es zu vernichten. Schreiben und Unterlagen, die einem Adressaten in seiner Funktion als Mitglied eines kommunalen Vertretungsorgans zugehen, sind keine privaten Dokumente, sondern Verwaltungsunterlagen.

Ferner hat der ehemalige Stadtvertreter gegen die nach § 23 Abs. 6 Kommunalverfassung für das Land Mecklenburg-Vorpommern (KV M-V) geltende Verschwiegenheitspflicht verstoßen. Hiernach hat ein Gemeindevertreter regelmäßig über alle ihm im Rahmen seiner Tätigkeit bekannt gewordenen Angelegenheiten Stillschweigen zu wahren. Lediglich soweit Tatsachen offenkundig sind oder ihrer Bedeutung nach keine Geheimhaltung erfordern, dürfen diese offenbart werden. Gemäß § 23 Abs. 6 Satz 4 KV M-V besteht die Verschwiegenheitspflicht auch nach Beendigung der Tätigkeit als Gemeindevertreter fort.

Sowohl der Vorsitzende der Stadtvertretung als auch der Oberbürgermeister haben im Ergebnis mitgeteilt, dass den Stadtvertretern die datenschutzrechtlichen Bestimmungen bekannt sind. Gleichzeitig sicherten sie zu, dass die datenschutzrechtlichen Vorschriften künftig eingehalten werden.

Ich habe ein Arbeitspapier zu datenschutzrechtlichen Fragen in kommunalen Vertretungen erstellt, welches kostenlos bei mir angefordert werden kann.

3.7.2 Veröffentlichungen in der Gemeinde

Informationen über Rechtsstreitigkeiten

Ein Bürgermeister informierte die Einwohner im amtlichen Bekanntmachungsblatt über die erledigten und laufenden Rechtsstreitigkeiten der Gemeinde. Dieser Veröffentlichung war beispielsweise zu entnehmen, dass ein Mitarbeiter der Verwaltung erfolglos gegen seine Entlassung geklagt hatte und dass der arbeitsrechtliche Streit mit einer anderen Mitarbeiterin über die Arbeitsplatzbewertung sowie zwei weitere Streitigkeiten mit Betroffenen über die Höhe ihrer Honorarforderungen durch Vergleiche beigelegt werden konnten. Eine Einwohnerin war in zwei mietrechtlichen Auseinandersetzungen gegenüber der Gemeinde erfolgreich. Ferner hatte die Gemeinde in einem Fall Strafanzeige wegen Veruntreuung erstattet. Die einzelnen betroffenen Personen wurden namentlich genannt.

Der Bürgermeister vertrat die Auffassung, dass diese Veröffentlichung zulässig sei. Dies ergäbe sich aus dem Grundsatz der Öffentlichkeit von gerichtlichen Verhandlungen gemäß § 169 Gerichtsverfassungsgesetz. Da die Verhandlungen regelmäßig öffentlich sind, hätte ohnehin jeder die Möglichkeit, die Daten der Beteiligten zur Kenntnis zu nehmen.

Es trifft zu, dass bei öffentlichen Gerichtsverhandlungen Dritte regelmäßig personenbezogene Daten der am Verfahren Beteiligten erfahren. Jedoch ist zu berücksichtigen, dass es sich um eine „begrenzte Öffentlichkeit“ handelt. Der Öffentlichkeitsgrundsatz im gerichtlichen Verfahren gibt den Anwesenden die Möglichkeit, den ordnungsgemäßen Ablauf des Verfahrens und die Wahrung der Rechte der Beteiligten zu kontrollieren. Damit ist zwangsläufig die Bekanntgabe der im Verfahren relevanten, auch personenbezogenen Daten verbunden. Daraus folgt jedoch nicht das Recht, einer Stadt, einer bestimmten Region oder gar weltweit sämtliche personenbezogenen Daten der Verfahrensbeteiligten bekannt zu geben. Es ist zu unterscheiden, ob jemand an der Verhandlung vor Ort als Besucher teilnimmt oder ob die Daten auch für alle anderen nicht anwesenden Personen durch Veröffentlichungen „frei Haus“ geliefert werden. Auch Gerichtsurteile werden nur in anonymisierter Form veröffentlicht, um die Persönlichkeitsrechte der Beteiligten zu wahren. Bei den laufenden Verfahren war darüber hinaus auch zu berücksichtigen, dass noch nicht in allen Fällen eine Verhandlung stattgefunden hatte und somit noch nicht einmal eine „begrenzte Öffentlichkeit“ hergestellt worden war.

Der Hinweis auf die öffentlichen Gerichtsverhandlungen rechtfertigte daher keine Bekanntgabe der personenbezogenen Daten durch eine öffentliche Stelle. Dafür wäre eine Rechtsgrundlage erforderlich. Der Bürgermeister hat gemäß § 16 Kommunalverfassung für das Land Mecklenburg-Vorpommern (KV M-V) die Aufgabe, die Einwohner über allgemein bedeutsame Angelegenheiten zu informieren. Für diesen Zweck hätte es jedoch genügt, die Informationen in allgemeiner Form, ohne namentliche Nennung der Betroffenen, zu geben. Ein weitergehendes öffentliches Interesse bestand in diesem Fall nicht. Die Veröffentlichung war unzulässig. Die schutzwürdigen Belange der Betroffenen sind nicht beachtet worden.

Der Bürgermeister hat zugesagt, künftig keine personenbezogenen Übersichten mehr zu veröffentlichen.

Tagungsordnungspunkte des nichtöffentlichen Teils von Sitzungen

Eine Stadt hatte die Tagesordnungspunkte des nichtöffentlichen Teils einer Ausschusssitzung mit personenbezogenen Daten in der Tageszeitung veröffentlicht. Die Leser konnten der Veröffentlichung entnehmen, wer einen Pacht- bzw. Kaufvertrag für ein bestimmtes Grundstück abschließen oder wer an seinem Haus noch etwas anbauen wollte. In einem anderen Fall veröffentlichte eine Stadt die Tagesordnung für den nichtöffentlichen Teil der Stadtvertretersitzung mit dem Namen eines Betroffenen im Zusammenhang mit einer Disziplinarangelegenheit.

Bei der Erörterung mancher Angelegenheiten müssen Gemeindevertreter auch mit personenbezogenen Daten umgehen. Da die Sitzungen der Gemeindevertretung grundsätzlich öffentlich sind, ist in diesen Fällen gemäß § 29 Abs. 5 Satz 2 KV M-V zu prüfen, ob überwiegende schutzwürdige Belange der Betroffenen einen Ausschluss der Öffentlichkeit erfordern und die Angelegenheit in nichtöffentlicher Sitzung zu behandeln ist (siehe hierzu Dritter Tätigkeitsbericht, Punkt 3.7.1).

Die Tagesordnungspunkte für den nichtöffentlichen Teil von Sitzungen der Gemeindevertretungen und deren Ausschüsse sind nach § 29 Abs. 6 und § 36 Abs. 6 KV M-V so bekannt zu geben, dass der Zweck des Ausschlusses der Öffentlichkeit nicht gefährdet wird. Dies kann regelmäßig durch eine allgemeine Beschreibung des Gegenstandes, wie Personal- oder Grundstücksangelegenheit, erreicht werden. Bei der Veröffentlichung der in diesem Sitzungsteil gefassten Beschlüsse ist dies gemäß § 31 Abs. 3 und § 36 Abs. 6 KV M-V ebenfalls zu berücksichtigen.

In beiden Fällen habe ich die Veröffentlichungspraxis geprüft und festgestellt, dass es sich um einzelne datenschutzrechtliche Verstöße handelte. Die Städte sicherten zu, künftig sorgfältiger zu verfahren.

3.7.3 Umgang mit personenbezogenen Daten bei Rechnungsprüfungen

Ein Landrat hat mich um datenschutzrechtliche Hinweise zur Behandlung von Rechnungsprüfungsberichten im Kreistag gebeten. Folgendes habe ich empfohlen:

Personenbezogene Daten, die öffentliche Stellen für bestimmte Zwecke im Rahmen ihrer gesetzlichen Aufgabenerfüllung erheben, verarbeiten und nutzen, dürfen gemäß § 9 Abs. 4 DSGVO auch für die Rechnungsprüfung in dem dafür erforderlichen Umfang genutzt werden. Der Zugriff auf diese Daten ist jedoch nur zulässig, soweit er

unerlässlich oder unvermeidbar ist. Das ist der Fall, wenn die Rechnungsprüfung nicht ohne die personenbezogenen Daten durchgeführt werden kann. Unter diesen Voraussetzungen darf die Rechnungsprüfungsbehörde auch Unterlagen mit personenbezogenen Daten einsehen und nutzen.

Bei der Darstellung der Prüfungsergebnisse im Bericht ist darauf zu achten, dass der Sachverhalt, soweit möglich, allgemein beschrieben und dass auf personenidentifizierende Angaben verzichtet wird. So ist es beispielsweise für die Aufgabenerfüllung der Kreistagsmitglieder nicht erforderlich, den Namen einer zu niedrig oder zu hoch eingestuften Angestellten zu erfahren. Vielmehr ist der Fall als solcher – die Tatsache der falschen Einstufung – unabhängig von der konkreten Person relevant. Ein Personenbezug kann mittels Aktenzeichen oder über eine Liste von der Rechnungsprüfungsbehörde hergestellt werden, wenn dies, beispielsweise für personalrechtliche Maßnahmen, erforderlich ist.

Enthält ein Rechnungsprüfungsbericht personenbezogene Daten, so sind die schutzwürdigen Belange der Betroffenen zu beachten. In diesem Fall hat der Rechnungsprüfungsausschuss beziehungsweise der Kreistag, soweit dieser die Angelegenheit an sich gezogen hat, den Bericht in nichtöffentlicher Sitzung zu beraten. Unabhängig davon sind die Mitglieder des Kreistages nach § 23 Abs. 6 Kommunalverfassung für das Land Mecklenburg-Vorpommern zur Verschwiegenheit verpflichtet und insbesondere nicht berechtigt, die Unterlagen mit personenbezogenen Daten an die Presse weiterzugeben, wie dies in der Vergangenheit vereinzelt vorkam (siehe Zweiter Tätigkeitsbericht, Punkt 2.8.1).

Im Ergebnis hat der Landrat die Mitglieder des Kreistages nochmals schriftlich auf ihre Verschwiegenheitspflicht hingewiesen.

3.7.4 Einbruch im Rechnungsprüfungsamt

Die Presse berichtete, dass im Rechnungsprüfungsamt einer Stadt eingebrochen und ein Server mit personenbezogenen Daten gestohlen wurde. Bei meiner daraufhin durchgeführten Kontrolle habe ich Folgendes festgestellt:

Das Rechnungsprüfungsamt war übergangsweise in einem Gebäude untergebracht, das erhebliche bauliche Defizite aufwies. Das Gebäude war mit Glastüren verschlossen und das Schloss der Eingangstür mit einem einfachen Schließzylinder versehen. Fenster und Türen im Erdgeschoss sowie die Flure und Räume in den übrigen Geschos-

sen waren nicht besonders gesichert. Es existierten im gesamten Gebäude weder Bewegungsmelder noch eine Einbruchmeldeanlage; eine Kontrolle außerhalb der Dienstzeiten durch einen Wachdienst gab es ebenfalls nicht. Der Zugang zum Serverraum war zwar auf einzelne Mitarbeiter beschränkt. Jedoch war dieser Raum über eine Teeküche zugänglich und nur mit einer einfachen Tür verschlossen.

Dateibesreibungen und Geräteverzeichnisse lagen zum Zeitpunkt der Kontrolle nicht vor. Auf dem gestohlenen Server befanden sich umfangreiche Datenbestände zu Prüfungen der vergangenen Jahre, darunter auch sensible personenbezogene Daten. Die Daten waren lediglich passwortgeschützt gespeichert. Ein derartiger Schutzmechanismus für das Betriebssystem kann allerdings nicht verhindern, dass die gestohlene Festplatte des Servers mit einem Fremdprogramm gelesen wird. Eine Sicherungskopie des Datenbestandes wurde in einem Panzerschrank aufbewahrt, so dass die Daten erfolgreich wiederhergestellt werden konnten. Die in diesem Gebäude aufbewahrten Akten waren ebenfalls durch keine besonderen Maßnahmen gesichert.

Wegen der fehlenden technischen und organisatorischen Maßnahmen zur Gewährleistung einer ordnungsgemäßen Zugangs-, Datenträger-, Zugriffs- und Organisationskontrolle gemäß § 17 Abs. 2 Nr. 1, 2, 5 und 10, Abs. 3 Landesdatenschutzgesetz von Mecklenburg-Vorpommern (DSG MV) zum Schutz der personenbezogenen Daten habe ich gemäß § 28 Abs. 1 DSG MV den Zustand beanstandet. Ich habe zahlreiche Empfehlungen zur Umsetzung datenschutzgerechter Maßnahmen gegeben, um den desolaten Zustand zu beheben und den Schutz der Daten sicherzustellen. Insbesondere waren Maßnahmen zur Gebäudesicherung zu veranlassen und ein Datenschutz- und Datensicherheitskonzept für die automatisierte Verarbeitung personenbezogener Daten zu erstellen.

Des Weiteren hatte ich dem Oberbürgermeister empfohlen zu prüfen, ob in anderen Teilen der Stadtverwaltung, soweit sie dezentral in ähnlichen Gebäuden untergebracht sind, die erforderlichen Datenschutz- und Datensicherheitskonzepte vorliegen, ob die daraus resultierenden Maßnahmen umgesetzt wurden und ob eine sichere Aufbewahrung von Akten und sonstigen Unterlagen mit personenbezogenen Daten gewährleistet ist.

Der Bürgermeister hat meine Empfehlungen aufgegriffen und die erforderlichen Maßnahmen veranlasst.

3.8 Statistik

3.8.1 Empfehlungen zur Ausgestaltung einer Dienstanweisung für die kommunale Statistikstelle

Die Landkreise, kreisfreien Städte, Ämter und amtsfreien Gemeinden können zur Wahrnehmung ihrer Aufgaben statistische Erhebungen durchführen, soweit sie über eine kommunale Statistikstelle verfügen und ihnen nicht das Statistische Landesamt die erforderlichen Einzelangaben oder Ergebnisse zur Verfügung stellen kann. Die Einrichtung einer solchen Stelle ist ortsüblich bekannt zu geben sowie dem Landesamt, der jeweiligen Rechtsaufsichtsbehörde und dem Landesbeauftragten für den Datenschutz schriftlich anzuzeigen. Die kommunale Statistikstelle darf die Aufgaben der Kommunalstatistik allerdings erst dann wahrnehmen, wenn sie organisatorisch, räumlich und personell von den anderen Verwaltungsstellen der Kommune getrennt ist. In einer schriftlichen Dienstanweisung hat die Kommune die Maßnahmen festzulegen, die für die Abschottung dieses Bereiches von den anderen Stellen, für die statistische Geheimhaltung und für die Sicherung des Datenschutzes erforderlich sind. Dies ergibt sich aus §§ 10, 11 Landesstatistikgesetz.

Bisher haben nur die sechs kreisfreien Städte derartige Stellen eingerichtet. Bei Kontroll- und Informationsbesuchen habe ich festgestellt, dass die Abschottungsmaßnahmen sehr unterschiedlich und teilweise unzureichend sind. So kam es vor, dass statistische Erhebungen nicht von der Statistikstelle, sondern von anderen kommunalen Dienststellen durchgeführt wurden. Diese Situation ist auch darauf zurückzuführen, dass vorhandene Dienstanweisungen meist zu wenig Vorgaben für die ordnungsgemäße Wahrnehmung der Aufgaben der Statistikstelle enthalten.

Gemeinsam mit dem Statistischen Landesamt habe ich deshalb Empfehlungen zur Ausgestaltung einer Dienstanweisung „Statistik“ erarbeitet. Die Vorschläge enthalten detaillierte Regelungen zu den Aufgaben, zur Einrichtung und zu den erforderlichen organisatorischen und technischen Maßnahmen einer kommunalen Statistikstelle sowie zur Geheimhaltung und zum Datenschutz. Bei der Erarbeitung dieser Empfehlungen haben auch kommunale Statistikstellen, insbesondere der Leiter des Amtes für Statistik und Wahlen der Hansestadt Rostock, mitgewirkt. Der Entwurf wurde im Rahmen einer Sitzung des Arbeitskreises Statistik und Wahlen der kreisfreien Städte Mecklenburg-Vorpommern vorgestellt und mit den Leitern der kommunalen Statistikstellen überarbeitet.

Die Oberbürgermeister und Bürgermeister der kreisfreien Städte habe ich gebeten, ihre Dienstanweisungen den Empfehlungen entsprechend anzupassen. Anstatt einer Dienstanweisung kann auch eine (höherrangige) Satzung erlassen werden.

3.8.2 Wann wird die Hochbaustatistik datenschutzgerecht?

Für viele Entscheidungen in der Bau- und Wohnungspolitik werden präzise Informationen über die bauwirtschaftliche Entwicklung benötigt. Die für die Baustatistiken erforderlichen Daten werden bei den Kommunen, den Bauaufsichtsbehörden, den mit der Baubetreuung Beauftragten und bei den Bauherren erhoben. In unserem Land wird immer noch ein Erhebungsverfahren praktiziert, das aus folgenden Gründen nicht datenschutzgerecht ist:

- Das Verfahren basiert auf einem Runderlass des Innenministeriums vom 13. November 1992 (AmtsBl. M-V S. 1458). Der Erlass diente der Umsetzung des Zweiten Gesetzes über die Durchführung von Statistiken der Bautätigkeit und die Fortschreibung des Gebäudebestandes vom 27. Juli 1978 (BGBl. I S. 1118). 1999 ist das Hochbaustatistikgesetz vom 13. Mai 1998 (BGBl. I S. 869) in Kraft getreten und hat das Gesetz von 1978 abgelöst. Der Erlass hat damit keine gültige Rechtsgrundlage mehr.
- Der Erlass sieht unter anderem vor, dass die zuständige untere Bauaufsichtsbehörde die vom Bauherren gelieferten statistischen Angaben kontrolliert und gegebenenfalls selbst vervollständigt oder korrigiert. Das stellt einen schwer wiegenden Verstoß gegen den Grundsatz der Trennung von Statistik und Verwaltungsvollzug dar.
- Obwohl die Bauaufsichtsbehörden keine statistischen Erhebungsstellen sind, erhalten sie teilweise Kenntnis von statistischen Einzeldaten der Bauherren, die sie für ihre Arbeit nicht benötigen.

Im Jahr 2000 hat das Statistische Landesamt einen mit mir abgestimmten Entwurf für einen neuen Erlass zur Durchführung der Hochbaustatistik erstellt. Dieser liegt seit Februar 2001 dem Innenministerium vor. Es ist zu hoffen, dass der Erlass von 1992 bald durch einen neuen ersetzt wird, der sowohl den Belangen der Statistik als auch denen des Datenschutzes gerecht wird.

3.9 Telekommunikation und Medien

3.9.1 Telekommunikations-Überwachungsverordnung

Zwei Jahre nach dem ersten Entwurf hat die Bundesregierung am 24. Oktober 2001 die „Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (TKÜV)“ beschlossen. Rechtsgrundlage für die Verordnung ist § 88 des Telekommunikationsgesetzes (TKG) – Technische Umsetzung von Überwachungsmaßnahmen. § 88 TKG gibt die technischen Rahmenbedingungen für die Überwachung der Telekommunikation aufgrund der materiellen Vorschriften der Strafprozessordnung, des Gesetzes zu Artikel 10 Grundgesetz und des Außenwirtschaftsgesetzes vor. Die TKÜV regelt die hierfür erforderlichen technischen und organisatorischen Vorkehrungen und bestimmt den Kreis der Telekommunikationsanbieter, die verpflichtet sind, diese Maßnahmen auf eigene Kosten zu treffen.

In einer EntschlieÙung vom 10. Mai 2001 wandten sich die Datenschutzbeauftragten des Bundes und der Länder gegen den vom Bundesministerium für Wirtschaft Ende Januar 2001 vorgelegten Entwurf. Sie kritisierten die Aufnahme der Internetanbieter in den Kreis der Verpflichteten, weil damit eine technische Infrastruktur geschaffen würde, die jederzeit eine umfassende Überwachung des Internetverkehrs möglich macht (siehe Anlage 19).

Nach der nun erlassenen TKÜV sind die Internet-Provider zur Vorhaltung entsprechender Technik verpflichtet, wenn sie einen unmittelbaren teilnehmerbezogenen Zugang zum Internet anbieten. Darunter fallen zum Beispiel solche Unternehmen, die Internetzugänge über die Stromleitung, das Fernseekabelnetz oder breitbandige Netzanschlüsse, die einen besonders schnellen Internetzugriff ermöglichen, anbieten. Aber auch viele der übrigen Internet-Provider gehören zum Kreis der Verpflichteten, da sie E-Mail-Accounts anbieten und diese Dienstleistung in den Anwendungsbereich der TKÜV fällt. Insoweit muss leider festgestellt werden, dass die Kritik der Datenschutzbeauftragten nur zum Teil berücksichtigt wurde und mit einem umfangreichen Einsatz von Internet-Überwachungstechnik zu rechnen ist.

3.9.2 Evaluierung der Telekommunikationsüberwachung

Die Zahl der Telefonüberwachungen ist in den letzten Jahren sowohl bundes- als auch landesweit stark gestiegen. Die Datenschutzbeauftragten des Bundes und der Länder fordern allerdings schon seit langem eine Evaluierung der Überwachung der Telekommunikation, um Erfolg und Effizienz dieser Maßnahme hinterfragen zu können.

Im Jahre 1999 hat das Bundesministerium der Justiz ein entsprechendes Forschungsvorhaben beim Max-Planck-Institut für ausländisches und internationales Strafrecht in Auftrag gegeben. Dies haben die Datenschutzbeauftragten einhellig begrüßt. Inzwischen existiert auch durch die Verabschiedung des Strafverfahrensänderungsgesetzes am 2. August 2000 mit dem § 476 Strafprozessordnung eine ausreichende Ermächtigungsgrundlage, die die Übermittlung personenbezogener Informationen in Akten zu wissenschaftlichen Zwecken erlaubt. Damit sind zunächst die erforderlichen Voraussetzungen erfüllt.

Es bleibt abzuwarten, zu welchem Ergebnis die Untersuchung kommt.

3.9.3 Neue Medienordnung

Die technische Entwicklung und die Konvergenz der Medien machen es nahezu unmöglich, klare Grenzen zwischen Rundfunk, Medien- und Telediensten sowie Telekommunikation zu ziehen. Bund und Länder planen daher eine neue Medienordnung, die zu einer Vereinheitlichung der jeweiligen Rechtsvorschriften führen soll.

Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung vom Oktober 2001 (siehe Anlage 25) dazu aufgefordert,

- die Grundrechte auf Schutz der Privatsphäre, der Meinungsfreiheit und der Vertraulichkeit der Kommunikation zu beachten sowie
- das Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes zu einem medienunabhängigen allgemeinen Kommunikations- und Mediennutzungsgeheimnis weiter zu entwickeln und gesetzlich abzusichern.

Eine wichtige Rolle für die neue Medienordnung spielt das Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr vom 14. Dezember 2001 (siehe auch 3.17.2). Es beinhaltet unter anderem eine Novellierung des Teledienststedatenschutzgesetzes (TDDSG). Dazu gab es Überlegungen, die Anbieter von Telediensten zu verpflichten,

- die anfallenden Bestands- und Nutzungsdaten auch an Verwaltungsbehörden zur Verfolgung von Ordnungswidrigkeiten sowie an Nachrichtendienste zu übermitteln und
- die Nutzungsdaten auf Vorrat für eine mögliche spätere Strafverfolgung zu speichern.

Gegen diese Bestrebungen haben sich die Datenschutzbeauftragten in einer Entschließung vom März 2001 (siehe Anlage 14) gewandt, da sich anhand dieser Daten nachvollziehen lässt, wer mit wem kommuniziert hat und wer beim Surfen im Internet welchen Interessen nachgeht.

Die geplante Ausweitung der Übermittlungspflichten wurde nicht in das Gesetz übernommen. Dafür darf der Diensteanbieter nach dem neuen TDDSG Abrechnungsdaten statt bisher 80 Tage jetzt sechs Monate nach Rechnungsmonat speichern. Eine entsprechende Vorschrift findet sich auch in der Telekommunikations-Datenschutzverordnung (siehe Punkt 4.10). Es ist damit zu rechnen, dass eine solche Regelung künftig auch bei Mediendiensten gelten wird.

3.9.4 Datenübermittlung für die Rundfunkgebührenfinanzierung

Mit dem Ersten Gesetz zur Änderung des Gesetzes zum Staatsvertrag über den Norddeutschen Rundfunk vom 23. Juli 1998 (GVOBl. M-V S. 696) wurde die Rechtsgrundlage für eine regelmäßige Meldedatenübermittlung an den Norddeutschen Rundfunk (NDR) zum Zwecke der Rundfunkgebühreneinzahlung geschaffen. Aufgrund der datenschutzrechtlichen Bedenken (siehe hierzu Erster Tätigkeitsbericht, Punkt 2.3.2 und Zweiter Tätigkeitsbericht, Punkt 2.7.2) hat der Gesetzgeber diese Regelung zunächst bis zum 31. Dezember 2003 befristet. Der NDR hat sich gegenüber den Staatsvertragsländern verpflichtet, alle zwei Jahre einen Bericht zur Erforderlichkeit der regelmäßigen Datenübermittlung vorzulegen.

Der Inhalt des ersten Berichtes des NDR wurde gemeinsam mit dem Datenschutzbeauftragten und Mitarbeitern des NDR in konstruktiven Gesprächen erörtert. So wurde unter anderem festgestellt, dass das Merkmal „verheiratet oder nicht“ nur bei Sterbefällen benötigt wird. Die Gebühreneinzugszentrale wird den Meldebehörden kostenlos eine Verschlüsselungssoftware zur Verfügung stellen, um so die Voraussetzungen für eine sichere Übermittlung zu schaffen. Ich habe dem NDR empfohlen, den vorliegenden Bericht um die Ergebnisse dieser Gespräche zu ergänzen, um so eine Entscheidungsgrundlage für den Gesetzgeber zu erhalten.

Den Chef der Staatskanzlei habe ich über das Ergebnis informiert und ihm mitgeteilt, dass der NDR sich den datenschutzrechtlichen Aspekten mit besonderer Aufmerksamkeit widmet. Die regelmäßige Meldedatenübermittlung ist für den NDR zwar zu einem wichtigen Hilfsmittel geworden, um unberechtigte Abmeldungen zu vermeiden und neue Rundfunkteilnehmer zu gewinnen. Zu konstatieren bleibt jedoch, dass eine Vielzahl personenbezogener Daten verarbeitet werden muss, sofern das jetzige Verfahren beibehalten wird. Da derzeit noch nicht absehbar ist, ob das Instrumentarium der regelmäßigen Meldedatenübermittlung auch langfristig für eine erfolgreiche Rundfunkgebühreneinzug erforderlich ist, habe ich der Staatskanzlei unter anderem empfohlen, dass der NDR auch künftig regelmäßig über den weiteren Verlauf der Bestandsentwicklung berichten sollte.

Seit längerem gibt es Überlegungen der Länder zur Neuordnung der Rundfunkgebührenerhebung. Die 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer Sitzung am 12. und 13. Oktober 2000 eine EntschlieÙung zur Datensparsamkeit bei der Rundfunkfinanzierung verabschiedet und darauf hingewiesen, dass dieser Aspekt bei der Entwicklung von neuen Konzepten in besonderem Maße zu berücksichtigen ist (siehe Anlage 9). Die Ministerpräsidenten der Bundesländer haben im Herbst 2001 beschlossen, dass die Rundfunkgebühr künftig haushaltsbezogen erhoben werden soll. In die weiteren Überlegungen zu diesem neuen Modell sollten die Grundsätze der Datenvermeidung und der Datensparsamkeit einbezogen werden.

3.9.5 Konvention über Datennetzkriminalität

Der Europarat hat zusammen mit Japan, Kanada, Südafrika und den USA eine Konvention über Datennetzkriminalität (Cybercrime-Konvention) entworfen. Die Konvention verpflichtet die unterzeichnenden Staaten,

- die Strafvorschriften für Datennetzkriminalität und damit zusammenhängende Handlungen zu harmonisieren und gegebenenfalls zu erweitern,
- Befugnisse zur effektiven Ermittlung und Verfolgung der Datennetzkriminalität und solcher Straftaten zu schaffen, die mit Mitteln der Computertechnik begangen werden,
- eine schnelle und wirkungsvolle internationale Zusammenarbeit in diesem Bereich aufzubauen.

Am 23. November 2001 haben die meisten Mitgliedstaaten des Europarates, auch Deutschland, und die vier beteiligten außereuropäischen Staaten die Konvention unterzeichnet. Sie tritt in Kraft, wenn mindestens fünf Staaten, darunter drei Mitgliedstaaten des Europarates, sie ratifiziert haben. Der Text der Konvention, der Stand der Ratifikation sowie weitere Informationen des Europarates zur Konvention sind im Internet unter [http://conventions.coe.int/Treaty/ EN/projets/FinalCybercrime.htm](http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm) abrufbar.

In einer EntschlieÙung vom März 2001 haben die Datenschutzbeauftragten des Bundes und der Länder anlässlich des Entwurfes der Konvention unter anderem gefordert, dass bei der Schaffung von nationalen und internationalen Regelungen zur Bekämpfung von Datennetzkriminalität der Datenschutz und das Fernmeldegeheimnis gewährleistet werden sowie Daten von Internet-Nutzenden nur in Staaten mit angemessenem Datenschutzniveau übermittelt werden dürfen (siehe Anlage 14). Schon in der EntschlieÙung „Für eine freie Telekommunikation in einer freien Gesellschaft“ vom März 2000 haben die Datenschutzbeauftragten die Geltung des Fernmeldegeheimnisses auch im Bereich der Tele- und Mediendienste betont sowie Möglichkeiten zur anonymen und pseudonymen Nutzung des Internet verlangt (siehe Anlage 5).

Diese datenschutzrechtlichen Belange sind in der Konvention nicht berücksichtigt worden. Vielmehr ist festzustellen, dass materielle Bestimmungen zum Datenschutz oder zum Fernmeldegeheimnis fehlen, dass Rechtshilfeersuchen anderer Staaten keinerlei Einschränkungen zum Schutz der Betroffenen unterliegen und dass den Betroffenen kein Rechtsschutz bei der Übermittlung ihrer Daten garantiert wird. Insbesondere angesichts des geringen Datenschutzniveaus einiger Vertragsstaaten ist daher zu befürchten, dass die Konvention, wenn sie ratifiziert ist, zu einer Ausweitung der Speicherung und Übermittlung von Verbindungs- und Nutzungsdaten führt. Dies würde dann im Widerspruch zu den Datenschutzprinzipien des Europarates und erst recht zu denen der EU und Deutschlands stehen.

3.10 Finanzwesen

3.10.1 Pannen bei der Elektronischen Steuererklärung

Bereits im letzten Berichtszeitraum hatte ich festgestellt, dass das Projekt Elektronische Steuererklärung (ELSTER), welches in kommerziellen Steuersoftwarepaketen umgesetzt ist, weitgehend den datenschutzrechtlichen Anforderungen entspricht (siehe Vierter Tätigkeitsbericht, Punkt 3.9.7).

Im Frühjahr 2001 wurde ELSTER jedoch in der Zeitschrift Finanztest kritisiert. Die Steuerverwaltung des Bundes und der Länder hatte neben den kommerziellen Anbietern mit der Software „ElsterFormular 2000“ ein eigenes Programm angeboten, mit dem Steuerformulare elektronisch ausgefüllt und an das zuständige Finanzamt geschickt werden konnten. Das Programm selbst hatte keine Schwachstellen und entsprach dem Stand der Technik. Die Daten wurden beispielsweise mit anerkannten kryptographischen Verfahren wie Triple-DES und RSA 1024 angemessen geschützt.

Kritikwürdig war jedoch die Art und Weise, wie Steuerpflichtige das Programm erhalten sollten. Die Originalsoftware und die jeweils erforderlichen Updates wurden im Internetangebot der Steuerverwaltung zum Abruf bereitgehalten. Ein Steuerpflichtiger, der das Programm zur eigenen Nutzung heruntergeladen hat, konnte sich jedoch nicht völlig sicher sein, dass er tatsächlich das Originalprogramm der Steuerverwaltung bekommen hat. Es war nicht auszuschließen, dass Hacker den Server der Steuerverwaltung nachbilden und ein Programm zum Herunterladen anbieten, das für den Steuerpflichtigen vom Original zwar nicht zu unterscheiden ist, die von der Steuerverwaltung vorgesehenen Sicherheitsmechanismen jedoch nicht enthält. Wäre es Hackern gelungen, Steuerpflichtigen ein solches gefälschtes Programm unterzuschieben, wären Vertraulichkeit und Integrität der Steuerdaten nicht mehr sichergestellt.

Nachdem die Mängel bekannt geworden waren, hat die Steuerverwaltung „ElsterFormular 2000“ sofort vom Netz genommen. Sie ergänzte umgehend die erforderlichen Sicherheitsmaßnahmen, die unter anderem auch vom Bundesamt für Sicherheit in der Informationstechnik empfohlen worden waren.

Im Mai 2001 stand „ElsterFormular 2000“ wieder zum Abruf bereit. Ein Download war nun nur noch von einer zertifizierten Webseite der Steuerverwaltung unter Nutzung des besonders sicheren https-Protokolls mit 128 Bit Verschlüsselung möglich. Der Steuerpflichtige kann sich nun vor dem Herunterladen des verschlüsselten Programms davon überzeugen, dass er tatsächlich den Server der Steuerver-

waltung angewählt hat. Auf ebenso sichere Weise können bei Bedarf die Updates der Software geholt werden. Darüber hinaus wird das Programm „ElsterFormular 2000“ elektronisch unterschrieben (digitale Signatur). Bevor der Steuerpflichtige das Programm auf dem eigenen Rechner installiert, muss er sich eine zweite Software herunterladen, mit der er zunächst prüft, ob die digitale Signatur gültig ist. Mit diesen, dem Stand der Technik entsprechenden Sicherheitsmaßnahmen bestehen auch aus datenschutzrechtlicher Sicht keine Bedenken, das Programm „ElsterFormular“ zu verwenden.

3.10.2 Fremdenverkehrsabgabe

Betroffene Bürger und Institutionen haben mich gebeten, die Zulässigkeit des Umgangs mit personenbezogenen Daten bei der Einführung einer Fremdenverkehrsabgabe in einer Stadt zu prüfen.

Ich habe festgestellt, dass das Verfahren in folgenden Punkten nicht datenschutzgerecht war:

Unter Hinweis auf § 31 Abgabenordnung (AO) sollte das örtliche Finanzamt Umsatzdaten der ansässigen Unternehmen an die Stadt übermitteln. Die Daten waren als Grundlage für die Kalkulation zum Aufkommen der Fremdenverkehrsabgabe gedacht. Das Finanzamt ist dem Ansinnen der Stadt zu Recht nicht gefolgt, da § 31 AO eine Übermittlung von Besteuerungsgrundlagen nur für die Festsetzung von Abgaben zulässt, nicht jedoch für Kalkulationen zur Vorbereitung von abgaberechtlichen Vorschriften. Als anfragende Stelle trägt die Stadt nach § 12 Abs. 2 Satz 2 Landesdatenschutzgesetz von Mecklenburg-Vorpommern (DSG MV) die Verantwortung für die Zulässigkeit der Datenübermittlung und somit auch für die Zulässigkeit des Ersuchens. Daher hätte sie bereits vor dem Ersuchen prüfen müssen, ob die entsprechenden Voraussetzungen vorliegen. Offensichtlich hatte sie es in diesem Fall versäumt.

Die Stadt schätzte daraufhin die Umsätze, ordnete sie auf einer Liste einzelnen Unternehmen zu und gab diese allen Fraktionen der Bürgerschaft zur Kenntnis. Diese Weitergabe war jedoch nicht erforderlich. Vielmehr hätte es ausgereicht, die Ergebnisse zusammenfassend darzustellen und das Verfahren für die Mitglieder der Bürgerschaft transparent zu gestalten.

Mit der Beschlussvorlage zur Fremdenverkehrsabgabe wurden die Abgeordneten der Bürgerschaft auch über die Kosten für Veranstaltungen einschließlich der gezahlten

Honorare und deren Empfänger informiert. Das war nach Auffassung des Oberbürgermeisters notwendig, um dem Informationsanspruch der Kommunalvertreter nach § 23 der Kommunalverfassung für das Land Mecklenburg-Vorpommern (KV M-V) hinreichend Rechnung zu tragen. Nur so könnten sie die zu erwartenden Ausgaben für den Fremdenverkehr einschätzen und den Abgabenmaßstab festlegen. Werden personenbezogene Daten genutzt und verarbeitet, ist nach § 10 DSGVO immer auch zu prüfen, ob diese Daten im Einzelfall für den Zweck tatsächlich erforderlich sind. Hier wäre es ausreichend gewesen, die Bürgerschaft in allgemeiner Form über die Ausgaben im Zusammenhang mit fremdenverkehrsfördernden Maßnahmen zu informieren, ohne die einzelnen Empfänger konkret zu nennen. Einer solchen Anonymisierung der Daten stand auch kein unverhältnismäßig hoher Aufwand im Sinne von § 10 Abs. 3 Satz 1 DSGVO entgegen.

Darüber hinaus wurden die Unterlagen mit personenbezogenen Daten auch an die Presse weitergegeben. Es lag somit ebenfalls ein Verstoß gegen das Datengeheimnis nach § 5 DSGVO beziehungsweise gegen die den Stadtvertretern obliegende Verschwiegenheitspflicht gemäß § 23 Abs. 6 KV M-V vor. Ungeklärt blieb, ob ein Mitarbeiter der Verwaltung oder ein Mitglied der Bürgerschaft die Daten weitergegeben hatte.

Aufgrund der im Verfahren aufgetretenen datenschutzrechtlichen Mängel habe ich den Vorgang nach § 28 Abs. 1 DSGVO beanstandet und Empfehlungen zu einer datenschutzgerechten Verfahrensweise gegeben. Der Oberbürgermeister hat in seiner Stellungnahme zugesagt, meine Hinweise zu berücksichtigen und künftig die datenschutzrechtlichen Belange genauer zu prüfen. Bei Beschlussvorlagen soll in besonderem Maße darauf geachtet werden, ob und inwieweit ein Umgang mit personenbezogenen Daten erforderlich ist.

3.10.3 Nutzung von Hundesteuerdaten für ordnungsbehördliche Zwecke?

Mit der Verordnung über das Führen und Halten von Hunden (Hundehalterverordnung – HundehVO M-V) vom 4. Juli 2000 (GVOBl. M-V S. 295) wurden Regelungen zum Schutz vor gefährlichen Hunden geschaffen. In diesem Zusammenhang hatte das Ordnungsamt einer Stadt das dortige Steueramt gebeten, ihm die Daten von Hundehaltern mit den Angaben zur Hunderasse mitzuteilen. Die Daten sollten für Aufgaben nach der Hundehalterverordnung genutzt werden. Da das Steueramt die Daten der Hundehalter jedoch für steuerrechtliche Zwecke speichert, hatte es wegen der

fehlenden Rechtsgrundlage datenschutzrechtliche Bedenken gegen die Weitergabe dieser Daten. Der behördliche Datenschutzbeauftragte der Stadt bat mich um eine datenschutzrechtliche Bewertung des Sachverhaltes.

Auch beim Umgang mit Hundesteuerdaten ist das Steuergeheimnis gemäß § 30 Abgabenordnung (AO) zu beachten. Daten dürfen nur dann an Stellen außerhalb der Steuerverwaltung übermittelt werden, wenn einer der in § 30 Abs. 4 AO genannten Offenbarungstatbestände erfüllt ist. Dies ist der Fall, wenn die Daten der Durchführung bestimmter, in der Abgabenordnung näher bezeichneter Verfahren dienen würden, eine anderweitige ausdrückliche gesetzliche Regelung existiert, der Betroffene zugestimmt hat oder ein zwingendes öffentliches Interesse besteht. Hier kommt allenfalls das zwingende öffentliche Interesse in Betracht. § 30 Abs. 4 Nr. 5 AO nennt Regelbeispiele, bei denen von einem zwingenden öffentlichen Interesse auszugehen ist. Eine Offenbarung der Daten ist hiernach nur zulässig, wenn die Gefahr besteht, dass ansonsten schwere Nachteile für das Allgemeinwohl eintreten würden. Somit kommen nur besonders bedeutsame und hinreichend konkrete Fälle in Betracht. Eine erhebliche Gefährdung kann zwar von einzelnen Hunden ausgehen, dies gilt jedoch nicht für die Mehrzahl der Hunde. Allein anhand der Steuerdaten ließe sich auch keine Differenzierung der Hunde vornehmen, es sei denn, einzelne Hundehalter hätten auf freiwilliger Basis das Merkmal „Hunderasse“ mitgeteilt. Aber auch in diesem Fall ist zu berücksichtigen, dass nicht ohne weiteres davon ausgegangen werden kann, dass die überwiegende Zahl der Hundehalter ihren Pflichten nach der Hundehalterverordnung nicht nachkommt. Entsprechende Erkenntnisse hierzu lagen jedenfalls nicht vor.

Da keiner der Offenbarungstatbestände nach § 30 Abs. 4 AO erfüllt ist, habe ich den behördlichen Datenschutzbeauftragten darüber informiert, dass ich seine Bedenken teile und eine Datenweitergabe in diesem Fall für unzulässig erachte.

3.10.4 PROFiskal

Für das zentrale Haushalts-, Kassen-, Rechnungswesenverfahren PROFiskal ist das Finanzministerium verantwortlich. Seit der Einführung des Verfahrens berate ich zu Datenschutzfragen bei der Planung, beim Betrieb und bei der Weiterentwicklung der Hard- und Softwarekomponenten (siehe Vierter Tätigkeitsbericht, Punkt 3.9.3). Schwerpunkt im Berichtszeitraum war dabei die Datensicherheit der Endgeräte bei den Anwendern. Hierfür existierte bislang kein IT-Sicherheitskonzept.

Die zentralen PROFiskal-Komponenten bei der DVZ M-V GmbH sind über ein Virtuelles Privates Netz (VPN) innerhalb des Landesdatennetzes LAVINE mit den Personalcomputern der Anwender verbunden, auf denen die dezentralen Programme ausgeführt werden. Auf diesen Endgeräten laufen in der Regel noch weitere Anwendungen. Dafür ist mitunter der Zugriff auf verschiedene andere Teilnetze innerhalb von LAVINE (z. B. LAPIS, WWW über die zentrale Firewall) oder innerhalb des Hausnetzes (z. B. Personalsoftware, internes Mailsystem) erforderlich. Ohne spezielle Sicherheitsmaßnahmen ist damit zu rechnen, dass sich eventuelle Störungen oder Manipulationen anderer Anwendungen oder Dienste auf PROFiskal auswirken.

Zudem wird PROFiskal nicht nur von Bediensteten aus dem Geschäftsbereich des Finanzministeriums genutzt. Dadurch war es bislang schwierig abzugrenzen, wer für welchen Teilbereich der Installation und Administration der Personalcomputer zuständig ist.

Um geeignete technische und organisatorische Maßnahmen zur Beseitigung der oben genannten Mängel festzulegen, hat das Finanzministerium ein IT-Sicherheitskonzept für die Endgeräte erarbeitet. Es enthält unter anderem folgende Lösungsansätze:

- Die sensiblen Verfahrensteile von PROFiskal werden über ein spezielles Terminalprogramm bedient. Dadurch unterscheiden sich die Protokolle des PROFiskal-Netzes von denen der anderen anwendungsspezifischen Netze. Es ist also eine Protokolltrennung möglich. Überdies ist die Terminal-Software recht einfach zu bedienen und zu pflegen.
- Vor der Einrichtung eines Arbeitsplatzes verpflichtet sich der Betreiber des PC schriftlich, die im Konzept vorgeschriebenen Rahmenbedingungen einzuhalten. Für die bereits existierenden Arbeitsplätze wird dies schrittweise nachgeholt.
- Die grundlegenden infrastrukturellen und baulichen Maßnahmen orientieren sich am IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Sie sind durch den Betreiber des Arbeitsplatzes zu realisieren.
- Für die Konfiguration von Betriebssystem und Netzwerk werden Vorgaben formuliert, die ebenfalls auf dem Grundschutzhandbuch beruhen. Der jeweilige Betreiber sowie das Finanzministerium können festgelegte Bereiche administrieren. Alle diese Aktionen werden protokolliert und bei Bedarf gemeinsam kontrolliert.

- Sollen an einem PROFiskal-Arbeitsplatz auch Internetdienste zur Verfügung stehen, so ist grundsätzlich die zentrale Firewall von LAVINE zu nutzen. Dezentrale Internetzugänge sind unzulässig.
- Die PROFiskal-Arbeitsplätze werden nicht vom Finanzministerium oder der DVZ M-V GmbH ferngewartet. Wird der PC durch den für den Arbeitsplatz Verantwortlichen oder einen Dritten ferngewartet, so darf dies nur innerhalb des lokalen Netzes oder innerhalb von LAVINE geschehen. Ist eine Übernahme von Bildschirm oder Eingabegeräten im Rahmen der Fernwartung vorgesehen, so bedarf dies der Zustimmung der betroffenen Bediensteten; diese sollen ihre PROFiskal-Anwendung vor der Übernahme schließen.

Das Sicherheitskonzept entspricht somit den allgemeingültigen Empfehlungen zur Nutzung verschiedener Anwendungen und Netze auf einem Endgerät (siehe Punkt 3.18.5), ist aber speziell auf die Anforderungen von PROFiskal zugeschnitten und baut auf Maßnahmen auf, die in LAVINE bereits realisiert sind.

3.10.5 Was darf das Finanzamt über das private Telefonieren oder Surfen am Arbeitsplatz wissen?

Das Bundesministerium der Finanzen hatte am 24. Mai 2000 in einem Schreiben an die obersten Finanzbehörden der Länder die steuerliche Behandlung der Telefonate und der Internetnutzung der Arbeitnehmer mit Wirkung ab dem Jahr 2001 neu geregelt. Um eventuelle steuerpflichtige geldwerte Vorteile zu ermitteln, hätten danach beispielsweise für alle Arbeitnehmer Einzelverbindungs-nachweise mit ungekürzten Zielrufnummern und Listen der aufgesuchten Websites erstellt werden müssen, sofern der Arbeitgeber das private Telefonieren oder Surfen am Arbeitsplatz zulässt.

Diese Verfahrensweise haben sowohl die Datenschutzbeauftragten des Bundes und der Länder als auch die Wirtschaft und Verwaltung aus folgenden Gründen abgelehnt:

- Die Pflicht zur Vorlage ungekürzter Einzelverbindungs-nachweise stellt einen unverhältnismäßigen Eingriff in das Telekommunikationsgeheimnis der betroffenen Gesprächsteilnehmer dar, für den keine gesetzliche Grundlage existiert.
- Das Verfahren steht im Widerspruch zur Telekommunikations-Datenschutzverordnung.

- Die geforderte Vollprotokollierung der Internetzugriffe verstößt gegen das Telemediendiensteschutzgesetz und den Mediendienste-Staatsvertrag.
- Immer mehr Behörden und Unternehmen nutzen Pauschaltarife ohne zeitliche oder mengenmäßige Begrenzung, so genannte Flatrates, bei denen sich der „private“ Anteil nicht mehr ermitteln lässt.
- Der erforderliche bürokratische Mehraufwand steht in keinem Verhältnis zu den zu erwartenden Steuereinnahmen.
- Schließlich konterkariert die Vorgehensweise das Bemühen der Bundesregierung, die Nutzung des Internet voranzutreiben.

Erfreulicherweise hat das Bundesministerium der Finanzen auf die Kritik reagiert und mit Schreiben vom 16. Oktober 2000 die Regelung wieder aufgehoben. In das Einkommensteuergesetz wurde Ende 2000 mit § 3 Nr. 45 sogar eine Bestimmung eingefügt, wonach „die Vorteile des Arbeitnehmers aus der privaten Nutzung von betrieblichen Personalcomputern und Telekommunikationsgeräten“ steuerfrei sind.

3.11 Soziales

3.11.1 Umgang mit Sozialdaten – immer wieder aktuell

Auch im vergangenen Berichtszeitraum habe ich verschiedene Anfragen von Bürgern zum Umgang mit Sozialdaten erhalten. Die Praxis zeigt, dass nach wie vor große Unsicherheit darüber besteht, welche Angaben das Sozialamt erheben darf. Die folgenden Beispiele sollen dies verdeutlichen.

Ein Petent informierte mich darüber, dass seine Bekannte beim Sozialamt Hilfe zum Lebensunterhalt beantragt hatte. Das Sozialamt lehnte jedoch ab, weil sie mit dem Petenten in einer eheähnlichen Gemeinschaft lebe. Der Lebenspartner wäre verpflichtet, Unterhalt zu leisten oder dazu beizutragen. Das Sozialamt begründete seine Entscheidung damit, dass der vermutete Lebenspartner sich nach Auskunft seiner Mitbewohner in seiner eigenen Wohnung nur selten aufhalte. Außerdem habe er in den letzten zwei Monaten für diese Wohnung keine Miete gezahlt.

Der Petent bat mich, den Sachverhalt datenschutzrechtlich zu prüfen. Insbesondere wollte er wissen, ob das Sozialamt „hinter seinem Rücken“ Daten über ihn erheben darf.

Grundsätzlich sind die Sozialleistungsträger verpflichtet, die für die Entscheidung erheblichen Tatsachen von Amts wegen zu ermitteln (§§ 20, 21 Sozialgesetzbuch Zehntes Buch – SGB X). Dabei können sie Art und Umfang der Ermittlung selbst bestimmen. Die Mittel hierfür müssen erforderlich, angemessen und verhältnismäßig sein. Das Sozialamt darf also nur die Tatsachen ermitteln, die für den konkreten Einzelfall notwendig sind und zum unmittelbaren Umfeld des Hilfeempfängers gehören. Im eingangs geschilderten Fall war es jedoch unverhältnismäßig, für die Beurteilung des Sachverhaltes personenbezogene Daten des vermuteten Lebenspartners bei Dritten zu erheben, die keinen unmittelbaren Bezug zu dem Sachverhalt haben.

Ich habe deshalb die Datenerhebung über den vermuteten Lebenspartner der Antragstellerin als unzulässig bewertet und empfohlen, künftig nur Daten zu erheben, die zweifelsfrei geeignet sind, eine eheähnliche Gemeinschaft nachzuweisen. Das Sozialamt hat mir mitgeteilt, dass es meine Empfehlungen berücksichtigen und das Ermessen im Umgang mit Sozialdaten enger auslegen wird. Den Petenten habe ich über das Ergebnis informiert.

In einem anderen Fall teilte mir ein Hilfeempfänger mit, dass das Sozialamt ihn aufgefordert habe, monatlich seine Kontoauszüge vorzulegen. Kopien der Auszüge

ge würden dann zur Sozialhilfeakte genommen. Der Petent wollte wissen, ob dies zulässig sei.

Ein Mitarbeiter des Sozialamtes bestätigte mir, dass alle Sozialhilfeempfänger in monatlichen Abständen Kontoauszüge vorlegen müssen, deren Kopien dann zur Akte genommen werden. Dieses Vorgehen resultiere aus der Mitwirkungspflicht der Hilfeempfänger (§§ 60 bis 67 Sozialgesetzbuch Erstes Buch – SGB I). Damit sollen alle Leistungen, die die betroffene Person erhält, kontrolliert werden.

Dieses Vorgehen habe ich für unzulässig erklärt. Das Ziel der Sozialhilfe, den Hilfeempfänger zu einem unabhängigen Leben zu befähigen, wird gerade nicht durch eine hohe Kontrollichte erreicht, in deren Ergebnis der betroffenen Person viele Entscheidungen abgenommen werden.

Sozialhilfe erhalten nur Personen, die ihren Lebensunterhalt nicht aus eigenen Mitteln bestreiten können. Das Sozialamt muss prüfen, ob diese Voraussetzung vorliegt. Bei dieser Prüfung hat es unter anderem sämtliche Einkünfte und das Vermögen der Antragsteller zu berücksichtigen. Grundsätzlich ist aber zunächst davon auszugehen, dass diese Angaben im Antrag vollständig und wahrheitsgemäß sind. Bestehen jedoch berechnete Zweifel, kann das Sozialamt entsprechende Beweismittel verlangen (§§ 20, 21 SGB X). Darüber hinaus sind die Antragsteller und Hilfeempfänger verpflichtet, bei der Ermittlung der entscheidungserheblichen Tatsachen mitzuwirken (§ 60 SGB I). Im Einzelfall können deshalb auch Kontoauszüge verlangt werden. Angemessen wäre dies, wenn erstmals laufende Leistungen beziehungsweise einmalige Beihilfen beantragt werden oder wenn konkrete Fragen zur Einkommens- und Vermögenssituation zu klären sind und dies nicht durch andere Unterlagen möglich ist. Auch wenn das Sozialamt Zweifel hat, ob die Angaben zum Einkommen vollständig und richtig sind, kann die betroffene Person aufgefordert werden, entsprechende Kontoauszüge vorzulegen. Dies kann beispielsweise der Fall sein, wenn konkrete Anhaltspunkte für einen Sozialhilfemissbrauch vorliegen.

Ich habe dem Sozialamt empfohlen, die Hinweise zur Vorlage von Kontoauszügen anzuwenden, die das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein mit dem Ministerium für Arbeit, Gesundheit und Soziales des Landes Schleswig-Holstein (veröffentlicht unter <http://www.datenschutzzentrum.de>) abgestimmt hat. Das Sozialamt hat meine Empfehlungen dem Landkreistag Mecklenburg-Vorpommern mit der Bitte übersandt, hierzu Stellung zu nehmen. Von dort wurde mir mitgeteilt, dass diese Hinweise künftig landesweit berücksichtigt werden.

3.11.2 Auszahlung der Vertriebenenzuwendung

Anfang des Jahres 2000 hat mich ein Bürger auf einen Zeitungsartikel aufmerksam gemacht. In diesem wurde berichtet, dass eine Stadt alle Antragsteller auf Vertriebenenzuwendung durch den Bundesbeauftragten für die Stasi-Unterlagen auf Mitarbeit im Ministerium für Staatssicherheit oder im Amt für Nationale Sicherheit überprüfen ließ.

Nach den Vorschriften des Vertriebenenzuwendungsgesetzes und den vom Innenminister unseres Landes dazu herausgegebenen Richtlinien ist eine Anfrage beim Bundesbeauftragten für die Stasi-Unterlagen nur im Einzelfall zulässig. Eine Einzelanfrage kommt in Betracht, wenn Anhaltspunkte dafür bestehen, dass Vertriebene vor oder nach dem Ende des Zweiten Weltkrieges einem totalitären System erheblich Vorschub geleistet oder durch ihr Verhalten gegen die Grundsätze der Menschlichkeit oder Rechtsstaatlichkeit verstoßen haben.

Ich habe die Verfahrensweise gegenüber dem Oberbürgermeister der Stadt beanstandet und den Innenminister unseres Landes darüber unterrichtet. Des Weiteren habe ich empfohlen, die Daten, die unter Verstoß gegen die oben genannten Vorschriften erhoben worden sind, nicht zu nutzen, sondern umgehend zu löschen. Bereits laufende Anfragen, zu denen der Bundesbeauftragte für die Stasi-Unterlagen noch nichts mitgeteilt hatte, sollte die Stadt zurückziehen. Zudem sollten die Betroffenen in geeigneter Weise über die Löschung informiert werden.

Der Oberbürgermeister ist meinen Empfehlungen gefolgt. Das Fachamt hat alle abgelehnten Entscheidungen erneut überprüft. Ich habe den Bürger, der mich auf den Sachverhalt aufmerksam gemacht hatte, entsprechend informiert.

3.11.3 Regelung zur Datenübermittlung zwischen Ärzten in der gesetzlichen Krankenversicherung

Anlässlich einer Tagung zur Telemedizin wollte ein Teilnehmer von mir wissen, wie eine in das Sozialgesetzbuch Fünftes Buch (SGB V) durch Gesetz vom 22. Dezember 1999 neu aufgenommene Rechtsvorschrift umzusetzen sei. Nach dieser Vorschrift (§ 73 Abs. 1 b SGB V) sind unter anderem Fachärzte oder andere Leistungserbringer verpflichtet, einen gesetzlich versicherten Patienten nach seinem Hausarzt zu fragen. Diesem sollen dann Behandlungsdaten und Befunde zu Doku-

mentationszwecken und für weitere Behandlungen übermittelt werden, wenn der Patient schriftlich eingewilligt hat. Ein Widerruf der Einwilligung ist möglich.

Der Teilnehmer berichtete, die Vorschrift werde in seinem Bereich gegenwärtig so umgesetzt, dass beispielsweise selbst bei einer Behandlung durch den Hausarzt und einer Mitbehandlung durch einen Facharzt Daten des Patienten zwischen beiden nur übermittelt würden, wenn die Einwilligung vorliegt. Dieses Vorgehen sei aber sowohl für die Ärzte als auch für die Patienten schwer nachvollziehbar. Ich habe ihm mitgeteilt, dass die Vorschrift so nicht auszulegen sei, und in diesem Zusammenhang auf die Berufsordnung der Ärztinnen und Ärzte in Mecklenburg-Vorpommern (BOÄ M-V) verwiesen. Dort heißt es, dass mehrere Ärzte, die einen Patienten gleichzeitig oder nacheinander untersuchen oder behandeln, von der Schweigepflicht befreit sind, wenn das Einverständnis des Patienten vorliegt oder anzunehmen ist (§ 9 Abs. 4 BOÄ M-V).

Vor diesem Hintergrund führen die folgenden Fallkonstellationen zu unterschiedlichen Zulässigkeitsvoraussetzungen für die Datenübermittlung:

Fall 1:

Ein Arzt benötigt die Dienstleistung eines anderen (Fach-)Arztes oder Leistungserbringers, um danach den Patienten weiter behandeln zu können. Der Patient erhält zu diesem Zweck in der Regel eine ärztliche Verordnung, welche die erforderliche Dienstleistung beschreibt. Eine Datenübermittlung vom behandelnden Arzt an den anderen Arzt/Leistungserbringer ist hierbei nicht erforderlich, da der Patient selbst entscheiden kann, welchen Arzt/Leistungserbringer er aufsucht. Die Ergebnisse der erbrachten Dienstleistung können dann an den behandelnden Arzt übermittelt werden. Der Patient muss nicht schriftlich einwilligen. Er wird auch davon ausgehen, dass die Ergebnisse für die Weiterbehandlung mitgeteilt werden. Anderenfalls hätte er der Datenübermittlung widersprochen.

Fall 2:

Ein Hausarzt überweist einen Patienten zur Fortsetzung und zum Abschluss der Behandlung an einen Facharzt oder Leistungserbringer. Der Hausarzt händigt dem Patienten entweder eine Überweisungsbescheinigung mit den erforderlichen Daten aus, die dieser dem von ihm gewählten Facharzt übergibt, oder der Patient bestimmt einen Facharzt, der die erforderlichen Daten erhalten soll. Eine förmliche schriftliche Einwilligung ist nicht notwendig, weil der Patient bestimmt, von welchem Arzt er weiter behandelt werden möchte. Ist die Behandlung bei dem Facharzt abgeschlossen, so besteht an sich kein Grund, dem Hausarzt darüber Näheres mitzuteilen. Dies war

nach der alten Rechtslage im SGB V auch nicht vorgesehen. Der Gesetzgeber wollte nun aber die Position des Hausarztes im Gesundheitswesen stärken und hat ihm dazu die Funktion des Koordinators übertragen. Zu diesem Zweck benötigt der Arzt umfassende medizinische Behandlungsdaten seines Patienten. Deshalb hat der Gesetzgeber die Datenübermittlung an den Hausarzt mit Einwilligung des Patienten geregelt (§ 73 Abs. 1 b SGB V).

Fall 3:

Ein Patient lässt sich von einem Facharzt/Leistungserbringer behandeln, ohne dass dies dem Hausarzt bekannt ist. Bei dieser Konstellation ist die Rechtsvorschrift des § 73 Abs. 1 b SGB V ebenfalls anzuwenden. Der Facharzt muss den Patienten nach seinem Hausarzt fragen und darf die Daten an diesen nur übermitteln, wenn der Patient einwilligt. Benötigt der Facharzt andererseits für seine Behandlung auch noch Daten vom Hausarzt oder von anderen Leistungserbringern, so kann er sie dort erheben, wenn der Patient einwilligt.

Im Juli 2001 teilte das Bundesministerium für Gesundheit dem Bundesbeauftragten für den Datenschutz mit, dass es in den Fällen, in denen der Versicherte mit der Übermittlung von Daten rechnen muss, in der Regel keiner schriftlichen Einwilligung bedarf. Damit wird die obige Auslegung unterstützt.

3.11.4 Behandlungsdaten an die Unfallkasse?

Die Unfallkasse Mecklenburg-Vorpommern hatte als gesetzlicher Unfallversicherungsträger bei einem Krankenhaus Krankenblätter einer Patientin angefordert. In dem Schreiben der Unfallkasse an das Krankenhaus hieß es unter anderem: „Sehr geehrter Herr Doktor, bitte übersenden Sie mir die Krankenblätter im Original in der o. g. Unfallsache zur Einsichtnahme.“ Das Krankenhaus hatte Zweifel, ob es die Daten auf dieser Grundlage an den gesetzlichen Unfallversicherungsträger übermitteln darf, und hat mich um Beratung gebeten.

Für die von der Unfallkasse erbetene Datenübermittlung sind die Bestimmungen des Sozialgesetzbuches Siebtes Buch (SGB VII) maßgeblich. Insbesondere die §§ 201 bis 203 enthalten hierzu nähere Regelungen. Danach haben Ärzte Daten über die Behandlung und den Zustand des Versicherten sowie andere personenbezogene Daten, die in diesem Zusammenhang erforderlich sind, an den Unfallversicherungsträger zu übermitteln (§ 201 Abs. 1 SGB VII), wenn sie eine Heilbehandlung aufgrund eines Unfalles durchführen, für den die gesetzliche Unfallversicherung Leistungen gewährt.

Nach der Vorschrift ist es somit zulässig, Gesundheitsdaten, die der ärztlichen Schweigepflicht unterliegen (§ 203 Abs. 1 Strafgesetzbuch – StGB), dem Unfallversicherungsträger für den gesetzlich bestimmten Zweck zu offenbaren.

Die Ärzte haben die versicherte Person unter anderem darüber zu informieren, dass sie gegenüber dem Unfallversicherungsträger zur Auskunft verpflichtet sind (§ 201 Abs. 1 Satz 5 SGB VII). Deswegen müsste ihnen die Vorschrift über ihre Auskunftspflicht bekannt sein. Dennoch ist es aus meiner Sicht sinnvoll, dass die Unfallkasse auf die Rechtsgrundlage für die Übermittlung hinweist, wenn sie die Daten bei einem Krankenhaus anfordert. Dies ergibt sich vor allem daraus, dass dieses Auskunftersuchen mitunter von einem anderen als dem behandelnden Krankenhausarzt beantwortet werden muss. Der Unfallkasse habe ich daher empfohlen, künftig die Rechtsgrundlage für die begehrte Datenübermittlung anzugeben. Dieser Empfehlung ist sie gefolgt.

Fraglich ist allerdings, ob die Unfallkasse regelmäßig die Originalunterlagen einsehen muss. Aus meiner Sicht müssen diese Unterlagen bei einem Leistungserbringer (z. B. Krankenhaus, Arzt) ständig verfügbar sein. Sie könnten beispielsweise benötigt werden, wenn eine weitere Behandlung erforderlich wird, die mit dem Unfall in einem medizinischen Zusammenhang steht. Der Vertreter der Unfallkasse teilte meine Auffassung, dass die Behandlungsoriginale grundsätzlich beim Arzt verbleiben sollen. Allerdings sei in den Bestimmungen des Abkommens Ärzte/Unfallversicherungsträger (Ärzteabkommen) vom März 1992 vereinbart worden, dem Arzt die Entscheidung zu überlassen, ob er das Original oder eine Abschrift liefert. Dagegen ist nichts einzuwenden. Sofern ein Arzt Originalunterlagen herausgibt, sollte er jedoch bedenken, dass die Dokumentation eines Behandlungsfalles zu seinen ärztlichen Berufspflichten gehört und er daher für einen etwaigen Verlust der Unterlagen vorsorgen muss, beispielsweise indem er selbst entsprechende Kopien behält.

Über die Rechtslage habe ich das Krankenhaus informiert.

3.11.5 Dürfen Sanitätshäuser Gesundheitsdaten ihrer Kunden erheben und übermitteln?

Nach den Vorstellungen einer Pflegekasse sollten alle Sanitätshäuser für ein bestimmtes Hilfsmittel Gesundheitsdaten ihrer Kunden erheben und an sie übermitteln. Die Pflegekasse wollte auf dieser Basis feststellen, ob das Hilfsmittel medizinisch notwendig und dessen Anwendung wirtschaftlich ist. Gegebenenfalls wollte sie den

behandelnden Arzt oder den Medizinischen Dienst der Krankenversicherung (MDK) konsultieren, um daraufhin eine schnelle Leistungsentscheidung treffen zu können. Dies hat sie den Sanitätshäusern so mitgeteilt. Es bestand die Vermutung, dass diese Datenerhebung und -übermittlung mit den datenschutzrechtlichen Bestimmungen nicht vereinbar sei.

Das Datenerhebungsformular trug die Überschrift: „Fragebogen zur Dekubitusversorgung“. Dekubitus- oder Durchliegeschwüre können bei pflegebedürftigen Menschen auftreten, die überwiegend im Bett liegen. Im Fragebogen wurden beispielsweise detaillierte Angaben zur Beschaffenheit der Haut der pflegebedürftigen Person verlangt. Es wurde auch gefragt, ob eine Allergie oder Inkontinenz vorliegt. Zudem sollten die Lage und die Größe der Dekubitusgeschwüre auf einer Körperskizze eingezeichnet werden.

Ich habe die Pflegekasse nach der Rechtsgrundlage für die Datenerhebung bei den Sanitätshäusern gefragt. Mir war insbesondere unklar, wie ein Sanitätshaus diese Daten erheben soll, wenn es zu der pflegebedürftigen Person möglicherweise gar keinen Kontakt hat. Denn solche Hilfsmittel werden in der Regel von Angehörigen oder einem Pflegedienst entgegengenommen.

Die Pflegekasse nannte als Rechtsgrundlage für die Datenerhebung das Sozialgesetzbuch Elftes Buch (SGB XI) – Soziale Pflegeversicherung, dort insbesondere die §§ 94 Abs. 1 Nr. 3 und 4, 28 Abs. 1 Nr. 5 in Verbindung mit § 40.

Ein Hilfsmittel kann in der gesetzlichen Pflegeversicherung von der betroffenen Person oder in ihrem Auftrag von einem Pflegedienst ohne eine ärztliche Verordnung beantragt und von der Kasse bewilligt werden. Es ist deshalb grundsätzlich nachvollziehbar, dass die Pflegekasse auch Gesundheitsdaten erhebt, damit sie feststellen kann, ob das Hilfsmittel notwendig ist. Pflegefachkräfte, die eine pflegebedürftige Person betreuen, seien aus ökonomischen Gründen in der Regel an Sanitätshäuser vertraglich gebunden. Deshalb habe sie sich an diese gewandt. Außerdem handele es sich hierbei um ein bundeseinheitliches Formular, weshalb sie auch das Verfahren der Datenerhebung mit ihrem Bundesverband und den darin vertretenen Pflegekassen der anderen Länder abstimmen wolle.

Im Ergebnis dieser Abstimmung teilte mir die Pflegekasse mit, dass sie meiner Empfehlung folgt und die Gesundheitsdaten künftig nicht mehr bei den Sanitätshäusern erhebt. Statt dessen wird eine Verfahrensweise eingeführt, die es erlaubt, im Zusammenwirken mit den Pflegefachkräften und den Ärzten zu klären, welche Art der Versorgung medizinisch notwendig und wirtschaftlich ist.

Das Sanitätshaus, das mich auf die Datenerhebung aufmerksam machte, habe ich über dieses Ergebnis informiert.

3.11.6 Nachweis des sozialen Status für eine ermäßigte Eintrittskarte

Ein arbeitsloser Petent teilte mir mit, dass ein Museum einen Arbeitslosenausweis verlangte, als er eine ermäßigte Eintrittskarte erwerben wollte. Zu Recht wies er den Kassierer darauf hin, dass es einen solchen Ausweis nicht gibt.

Ich habe beim Museum angefragt, wie eine arbeitslose Person nachweisen soll, dass sie die Voraussetzungen für diese ermäßigte Eintrittskarte erfüllt. Der Verwaltungsleiter sandte mir daraufhin die entsprechende Gebührenordnung zu. Darin wird keine besondere Bescheinigung gefordert. Dem Arbeitslosen ist es freigestellt, wie er den Ermäßigungsgrund nachweist. Ich habe den Petenten darüber informiert, dass das Museum beispielsweise eine vom Arbeitsamt ausgestellte Besucherkarte als Nachweis der Arbeitslosigkeit anerkennt.

Bedenklich allerdings war, dass die Gebührenordnung einen Sozialhilfeempfänger verpflichtet, den aktuellen Sozialhilfebescheid vorzulegen, wenn er eine ermäßigte Eintrittskarte kaufen will. Der Bescheid enthält aber neben den identifizierenden Angaben des Hilfeempfängers (Name, Vorname) auch solche über die Art der Hilfe sowie ihre Höhe. Die zuletzt genannten Informationen sind nicht erforderlich, um über die Ermäßigung zu entscheiden.

Ich habe dem Ministerium für Bildung, Wissenschaft und Kultur empfohlen, die Gebührenordnung so zu überarbeiten, dass auch Sozialhilfeempfänger eine ermäßigte Eintrittskarte erhalten können, ohne dafür den Sozialhilfebescheid vorlegen zu müssen. Dies ist auch vor dem Hintergrund zu sehen, dass einige Sozialämter entsprechende Bescheinigungen ausstellen, wenn Hilfeempfänger es wünschen. Die Bescheinigungen enthalten nur die wesentlichen identifizierenden Angaben und lediglich die Information, dass die Person Leistungen nach dem Bundessozialhilfegesetz bezieht. Das Ministerium hat zugesagt, meine Empfehlungen bei der nächsten Änderung der Gebührenordnung umzusetzen.

3.11.7 Risikostrukturausgleich in der gesetzlichen Krankenversicherung

Das Bundesministerium für Gesundheit hat einen Gesetzentwurf zur Reform des Risikostrukturausgleichs in der gesetzlichen Krankenversicherung erarbeitet. Dessen

Ziel ist es, eine bessere Datenbasis für Ausgleichszahlungen zwischen den Krankenkassen zu schaffen. Nach Auffassung des Ministeriums wird gegenwärtig die von chronisch Kranken verursachte Ausgabenbelastung einer Krankenkasse nur unzureichend berücksichtigt. Krankenkassen, in der viele chronisch kranke Personen versichert sind, sollen künftig eine Ausgleichszahlung von den Kassen erhalten, die nur wenige chronisch Kranke versichert haben. Zugleich werden in dem Gesetzentwurf Anreize für die Kassen geschaffen, Gesundheitsprogramme für chronisch kranke Personen zu entwickeln, so genannte Disease-Management-Programme.

Der Bundesbeauftragte und die Landesbeauftragten für den Datenschutz haben in einer gemeinsamen Stellungnahme unter anderem auf Folgendes hingewiesen:

- Die Berücksichtigung bestimmter versicherter Personen im Risikostrukturausgleich und die freiwillige Teilnahme an Disease-Management-Programmen bedeuten nicht zwingend, dass dafür mehr Sozialdaten (personenbezogene Daten) als bisher üblich verarbeitet werden müssen. Sollte dies jedoch erforderlich sein, wäre eine konkrete gesetzliche Regelung dafür notwendig. Die bewährte Trennung zwischen Daten für die Leistungsabrechnung, die bei den Krankenkassen, und Daten zur Dokumentation der Behandlung, die bei den Leistungserbringern gespeichert werden, sollte bestehen bleiben. Die Krankenkassen sollten darüber hinaus künftig nur pseudonymisierte Daten erhalten (siehe auch Punkt 3.11.7).
- Im Gesetzentwurf ist bisher nicht geregelt, wer für solche Gesundheitsprogramme der Krankenkassen werben darf. Wegen des wirtschaftlichen Interesses der Krankenkasse an einer hohen Teilnehmerzahl, die sich positiv auf die Ausgleichszahlungen auswirken würde, wäre eine Werbung durch sie selbst problematisch. Es ist insbesondere fraglich, ob bei einer Werbung durch die Krankenkasse von einer freiwilligen Teilnahme einer versicherten Person ausgegangen werden kann. Deshalb ist eine dies berücksichtigende gesetzliche Regelung erforderlich.
- Es sollte geregelt werden, wie zu verfahren ist, wenn eine versicherte Person ihre Teilnahme widerruft.
- Die vorgesehene Ergänzung der Krankenversichertenkarte um das Merkmal „chronisch kranke Person“ zur leichteren Erfassung der Daten dieser Gruppe im Risikostrukturausgleich hat erhebliche Auswirkungen für die Betroffenen. Wenn sie die Karte bei einem Leistungserbringer (z. B. der Physiotherapie, Orthopädie) vorlegen, offenbaren sie, dass sie dieser Gruppe angehören, ohne die Offenbarung vielleicht selbst zu wollen. Deshalb sollten Teilnehmer an Disease-Management-Programmen besser eine zusätzliche Patientenchipkarte erhalten.

Diese Hinweise und Empfehlungen sind im weiteren Gesetzgebungsverfahren beraten und zum großen Teil aufgenommen worden. Die Krankenversichertenkarte wird das Merkmal „chronisch kranke Person“ in einer Form enthalten, die gewährleistet, dass Dritte daraus keine Erkenntnisse gewinnen können.

Das Gesetz ist Ende Dezember 2001 verabschiedet worden. Es wird am 1. Januar 2002 in Kraft treten.

3.12 Gesundheitswesen

3.12.1 Innovatives Gesundheitsnetz Mecklenburg-Vorpommern

Im Juni des Jahres 2000 ist in Mecklenburg-Vorpommern das „Centrum für Angewandte Telemedizin Mecklenburg-Vorpommern“ (CAT M-V) als eingetragener Verein gegründet worden. Dieser Verein hat im Rahmen der durch die Landesregierung geförderten Multimediainitiative Mecklenburg-Vorpommern gemeinsam mit einem Telekommunikationsanbieter das „Innovative Gesundheitsnetz M-V“ (iGN M-V) ins Leben gerufen.

Über das Gesundheitsnetz sollen Patientendaten zwischen verschiedenen medizinischen Einrichtungen beziehungsweise Leistungserbringern übertragen werden, um die Patienten besser und effizienter behandeln zu können. Die erforderlichen Daten aus anderen Einrichtungen könnten sofort in eine aktuelle Behandlung einbezogen und dadurch beispielsweise aufwändige Doppel- oder Mehrfachuntersuchungen vermieden werden.

Die Verantwortlichen des Projekts haben um Beratung gebeten, um bereits in der Konzeptionsphase datenschutzrechtliche Bestimmungen und Empfehlungen berücksichtigen zu können. Ihnen ist bewusst, dass die Patienten das Gesundheitsnetz nur akzeptieren, wenn das besondere Vertrauensverhältnis zu den behandelnden Ärzten sich in adäquaten technischen und organisatorischen Maßnahmen widerspiegelt.

In der ersten Phase sollen vor allem Daten von Patienten verarbeitet werden, die einen hohen medizinischen Betreuungsbedarf in verschiedenen medizinischen Fachrichtungen haben. Das Netz wird zunächst in der Region Greifswald/Neubrandenburg etabliert. Im Wesentlichen sollen Krankenhäuser, niedergelassene Ärzte und Rehabilitationseinrichtungen die notwendigen Patientendaten untereinander übermitteln.

Bei den Beratungen habe ich auf Folgendes hingewiesen:

- Den Patienten muss es freigestellt sein, ob sie an dem iGN M-V teilnehmen wollen oder nicht. Entscheidet sich ein Patient für die Teilnahme, ist seine Einwilligung die Grundlage für die Verarbeitung der Daten im Netz.
- Auch ohne besondere Gründe ist es dem Patienten zu ermöglichen, die Teilnahme an dem Netz jederzeit zu beenden. Die Freiwilligkeit ist deshalb durch ein Wi-

derspruchsrecht des Patienten gegen die Verarbeitung seiner Daten im iGN M-V zu unterstützen. Folge eines Widerspruches ist, dass alle Daten gelöscht werden, die nicht bei einem behandelnden Arzt elektronisch gespeichert sind.

- Vor einer Einwilligung ist der Patient umfassend über die Verarbeitung der Daten im Gesundheitsnetz sowie über seine Rechte aufzuklären.

Neben diesen Grundvoraussetzungen sind durch weitere technische und organisatorische Maßnahmen die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und die Transparenz der Datenverarbeitung zu sichern. Beispielsweise dürfen übertragene Daten nicht verfälscht werden und müssen immer dem absendenden Arzt zugeordnet werden können. Dies wird durch die elektronische Signatur der zu übermittelnden Daten erzielt. Außerdem sind sie vor unberechtigter Kenntnisnahme durch Dritte zu schützen, was insbesondere durch kryptographische Verschlüsselung erreicht werden kann. Alle Verarbeitungsschritte sind darüber hinaus detailliert zu protokollieren.

Bisher sind diese Arbeiten auf einem guten Weg. Begünstigt wird die Entwicklung dadurch, dass auch die datenschutzrechtlichen Erfahrungen aus ähnlichen Projekten in anderen Bundesländern genutzt werden können.

3.12.2 Mustervertrag zum Umgang mit personenbezogenen Daten im Auftrag

Häufig übertragen öffentliche Stellen Aufgaben zur Verarbeitung personenbezogener Daten an Dienstleistungsunternehmen. So bedient sich beispielsweise ein Krankenhaus einer Servicegesellschaft, die als GmbH organisiert ist. Diese GmbH administriert, wartet und programmiert das Datenverarbeitungssystem.

Aus datenschutzrechtlicher Sicht handelt es sich dabei um eine Datenverarbeitung im Auftrag, die unter den Voraussetzungen des § 21 Landeskrankenhausgesetz für das Land Mecklenburg-Vorpommern zulässig ist (siehe auch Punkt 3.12.6.). Eine wesentliche Voraussetzung ist, dass zwischen dem Auftraggeber und dem Auftragnehmer ein schriftlicher Vertrag geschlossen wird, der das Nähere der Datenverarbeitung einschließlich der Kontrollrechte regelt.

Um öffentliche Stellen bei der datenschutzgerechten Vertragsgestaltung zu unterstützen, habe ich einen Mustervertrag zur Datenverarbeitung im Auftrag entworfen.

Dieser basiert auf den Ausarbeitungen meines hessischen Kollegen. Der Mustervertrag kann im Internet unter der Adresse www.lfd.m-v.de abgerufen werden.

3.12.3 Wer darf einen Krankenhausentlassungsbericht erhalten?

Es gab Anfragen, welche Stellen oder Personen einen Krankenhausentlassungsbericht (Epikrise) erhalten dürfen. Ein solcher Bericht wird in der Regel zum Abschluss einer Krankenhausbehandlung angefertigt und dokumentiert zusammenfassend die Behandlung eines Patienten. Der Bericht kann Vorschläge für eine weitere Behandlung enthalten.

Bei Gesprächen mit Krankenhausmitarbeitern habe ich festgestellt, dass sich bei der weiteren Verwendung der Epikrise ein gewisser Automatismus eingestellt hat. Häufig wird der Bericht nicht nur den Patientenunterlagen im Krankenhaus zugeordnet, sondern auch an den einweisenden Arzt, den Hausarzt und weiterbehandelnde Ärzte gesandt, ohne dass der Patient dies weiß oder der Datenübermittlung zugestimmt hat. Unter Umständen wird er sogar an die Krankenkasse weitergegeben, wenn diese ihn anfordert.

Die Krankenhäuser habe ich auf Folgendes hingewiesen: Nach dem Landeskrankenhausgesetz dürfen Patientendaten nur dann zu einer Mit- oder Nachbehandlung übermittelt werden, soweit es erforderlich ist und der Patient nichts anderes bestimmt hat (§ 17 Abs. 1 Nr. 2 LKHG M-V). Ist nach der Entlassung aus dem Krankenhaus eine weitere Behandlung erforderlich, sollte der Patient deshalb nach dem weiterbehandelnden Arzt gefragt und der Bericht an diesen nur versandt werden, wenn der Patient damit einverstanden ist. Beispielsweise kann das Einverständnis bei dem Entlassungsgespräch eingeholt werden. Die Frage nach dem Arzt ist erforderlich, weil der einweisende Arzt nicht der weiterbehandelnde Arzt sein muss. Ist der einweisende Arzt nicht weiter an der Behandlung beteiligt, darf er den Bericht nicht erhalten. Behandelt auch der Hausarzt nicht weiter, darf er die Epikrise nur dann bekommen, wenn der Patient eingewilligt hat (siehe auch Punkt 3.11.3 zu § 73 Abs. 1 b SGB V). Das Einverständnis des Patienten ist darüber hinaus ebenso in der Patientenakte zu dokumentieren wie die Angaben zum Datenempfänger.

Die Krankenhausmitarbeiter konnten diese Argumentation nachvollziehen und werden künftig entsprechend verfahren.

Weiterhin habe ich darauf hingewiesen, dass die Übermittlung des Krankenhausentlassungsberichtes an eine Krankenkasse nicht zulässig ist. Das Sozialgesetzbuch Fünftes Buch (SGB V) regelt die Verarbeitung von Sozialdaten und personenbezogenen Daten durch Krankenkassen. Die von einem Krankenhaus an eine Krankenkasse zu übermittelnden Daten sind in § 301 SGB V abschließend aufgeführt. Der Krankenhausentlassungsbericht ist in diesem Katalog nicht enthalten. Eine Krankenkasse hat grundsätzlich nur Anspruch auf die Daten, die erforderlich sind, um einen Leistungsanspruch zu begründen und eine Leistung abzurechnen. Die Daten in einem Krankenhausentlassungsbericht sind jedoch diesen Zwecken nicht zuzuordnen. Es handelt sich hierbei um solche Daten, die zur Behandlung eines Patienten gehören.

Der Bundesbeauftragte für den Datenschutz hat sich wegen der bundesweiten Bedeutung dieser Frage und wegen der bei ihm vorliegenden Eingaben zur Übermittlung von Krankenhausentlassungsberichten an Krankenkassen an die Bundesverbände der gesetzlichen Krankenkassen gewandt und sie darauf hingewiesen, dass sie den Bericht nicht verlangen dürfen. Eine Kopie dieses Schreibens habe ich den landesunmittelbaren gesetzlichen Krankenkassen sowie der Krankenhausgesellschaft und dem Sozialministerium zugesandt, um solche Datenübermittlungen in Mecklenburg-Vorpommern künftig auszuschließen.

3.12.4 Datenerhebung bei der Einschulungsuntersuchung

Eine Stadt beabsichtigte, einen Gesundheitsbericht zu erstellen, der den Zusammenhang von sozialem Umfeld und Gesundheit der Kinder zeigt. Die Ergebnisse sollten dazu beitragen, das kommunalpolitische Handeln auf dem Gebiet der Gesundheitsfürsorge und Gesundheitsvorsorge durch konkrete Empfehlungen zu unterstützen. Zu diesem Zweck wollte die Stadt den Datenerhebungsbogen für die Einschulungsuntersuchung um Angaben über die soziale Situation ergänzen. Diese zusätzlichen Daten und einige des ursprünglichen Erhebungsbogens sollten für den Gesundheitsbericht anonymisiert verarbeitet und genutzt werden. Der Kinder- und Jugendgesundheitsdienst der Stadt hat mich dazu um eine datenschutzrechtliche Stellungnahme gebeten.

Die Daten sollten zu unterschiedlichen Zwecken erhoben und verarbeitet werden – einerseits für die ärztliche Untersuchung und andererseits für den Gesundheitsbericht. Deshalb habe ich empfohlen, separate Formulare mit entsprechenden Erläuterungen über die Verarbeitung der Daten zu nutzen. Auch könnten so die Daten über die so-

ziale Situation bereits anonym erhoben werden, wenn auf identifizierende Daten des Kindes und seiner Eltern verzichtet und statt dessen lediglich der Stadtteil erfragt werden würde, in dem sie leben. Aus den weiteren Daten war kein Personenbezug herstellbar.

Der Kinder- und Jugendgesundheitsdienst der Stadt hat meine Empfehlungen umgesetzt. Die Eltern werden darüber aufgeklärt, dass die Beantwortung freiwillig ist und ihnen kein Nachteil entsteht, wenn sie die Fragen nicht beantworten, und dass der Fragebogen nicht den Gesundheitsunterlagen des Kindes zugeordnet wird.

Bei der Beratung zu dieser Angelegenheit habe ich festgestellt, dass der vor einiger Zeit mit mir abgestimmte Erhebungsbogen zur Schuleingangsuntersuchung erweitert worden ist. Die zusätzlichen Daten über die Krankheitsgeschichte des Kindes (Anamnese) sollen den Kinder- und Jugendarzt in die Lage versetzen, gezielter nach einer gesundheitlichen Störung zu suchen. Das Sozialministerium teilte mir mit, dass der Anamnesebogen aufgrund der fachlichen Einschätzung der Kinder- und Jugendärzte ergänzt worden sei. Die Ärzte hätten dargelegt, dass die zusätzlichen Daten erforderlich wären, um besser den Gesundheitszustand der Kinder beurteilen und bei gesundheitlichen Dispositionen geeignete Fördermaßnahmen empfehlen zu können.

Die Fragen über die Krankheitsgeschichte des Kindes sind auf freiwilliger Basis zu beantworten (die Teilnahme an den ärztlichen Untersuchungen zur Einschulung und während der Schulzeit ist allerdings gesetzlich vorgeschrieben – § 15 Abs. 2 Gesetz über den Öffentlichen Gesundheitsdienst – ÖGDG M-V). Die von mir dazu vorgeschlagene Formulierung zur Freiwilligkeit ist in das Informationsschreiben an die Eltern aufgenommen worden.

3.12.5 Einwilligung zur Speicherung im klinischen Krebsregister

In Mecklenburg-Vorpommern existieren vier klinische Krebsregister (Tumorzentren). Sie haben im Wesentlichen die Aufgabe, den an der Behandlung beteiligten Ärzten die erforderlichen Daten eines erkrankten Patienten zur Verfügung zu stellen, insbesondere um die Behandlung und die Nachsorge zu optimieren. Außerdem sollen die Daten für die regionale Krebsforschung genutzt werden. Darüber hinaus sind die Ärzte verpflichtet, Daten von Patienten mit Wohnsitz in Mecklenburg-Vorpommern an das Epidemiologische Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen, Sachsen-Anhalt und Thüringen zu übermitteln be-

ziehungsweise durch das Tumorzentrum übermitteln zu lassen (siehe auch Vierter Tätigkeitsbericht, Punkt 3.11.1).

Ärzte und Mitglieder der Krebsgesellschaft Mecklenburg-Vorpommern haben mich um Beratung zum Umgang mit Patientendaten durch die Tumorzentren gebeten. Nach ihrer Einschätzung sei die Datenbasis dieser Register ungenau und spiegele die tatsächlichen Erkrankungshäufigkeiten nicht wider. Dies resultiere vor allem daraus, dass Patienten bei einer Krebserkrankung unter Umständen in verschiedenen Kliniken behandelt werden und dadurch mehrfach registriert sein können. Für Forschungszwecke werden anonymisierte Daten genutzt, so dass sich bei einer Addition der Fallzahlen aus allen vier Tumorzentren eine höhere Anzahl an Erkrankten ergibt, als dies tatsächlich der Fall ist. Außerdem wären auch qualitative Aussagen über Behandlungen bisher nicht möglich, da sie nur durch so genannte Längsschnittuntersuchungen gewonnen werden können, bei denen der Krankheitsverlauf einer Person während der gesamten Behandlung beobachtet werden muss.

Konkret wollten die Ärzte wissen, wie unter Berücksichtigung der datenschutzrechtlichen Bestimmungen eine bessere Datenbasis erreicht werden kann, um zuverlässigere Ergebnisse über die Erkrankungshäufigkeit, die Erfolge der angewandten Therapien sowie über die Qualität der Behandlung zu gewinnen. Im Ergebnis der Beratung bestand Einigkeit darin, dass mit Einwilligung eines betroffenen Patienten seine Daten an die Klinik übermittelt werden können, in der er weiter behandelt wird, auch wenn die Behandlung zeitweilig unterbrochen war.

Die Krebsgesellschaft Mecklenburg-Vorpommern hat auf dieser Grundlage ein Informationsblatt entwickelt, das die behandelnden Ärzte den Patienten übergeben. Darin werden die Patienten umfassend über die Dokumentation ihrer Daten in einem der vier Tumorzentren und über ihre Rechte aufgeklärt. Der Unterschied zwischen einem klinischen und dem Epidemiologischen Register der fünf neuen Bundesländer in Berlin wird erklärt, und sie werden darauf hingewiesen, dass ihre Daten im klinischen Register nur gespeichert werden, wenn sie einwilligen. Patienten werden darüber hinaus auf Folgendes hingewiesen:

- Die Einwilligung ist freiwillig und kann jederzeit widerrufen werden,
- die Daten sind nur den behandelnden Ärzten zugänglich,
- die Daten werden in dem Register aktuell geführt, in dessen Bereich der Mittelpunkt der derzeitigen Behandlung liegt; wechselt ein Patient den Behandlungsmittelpunkt, können die Daten an das andere klinische Register übermittelt wer-

den, wenn der Patient dieser Datenübermittlung nicht widerspricht (dies entspricht auch der Regelung im Landeskrankenhausgesetz zur Datenübermittlung für eine Mit- oder Nachbehandlung),

- der Patient kann sein Recht auf Auskunft bei jedem behandelnden Arzt wahrnehmen,
- die gespeicherten Daten unterliegen nach wie vor der ärztlichen Schweigepflicht, dem Zeugnisverweigerungsrecht, dem Schutz vor Beschlagnahme und den datenschutzrechtlichen Bestimmungen des Landeskrankenhausgesetzes,
- die Daten können ohne Name und Adresse für die wissenschaftliche Forschung genutzt werden, dürfen aber nur in einer solchen Form veröffentlicht werden, die keinen Rückschluss auf die Person zulässt.

In diesem Zusammenhang haben Ärzte in Erwägung gezogen, die Einwilligungserklärung des Patienten zur Speicherung der Daten in einem klinischen Register in den Krankenhausaufnahmevertrag zu nehmen, um so die „Melderate“ für Krebserkrankungen zu erhöhen. Insbesondere sollte die Grundlage geschaffen werden, dass Pathologen ohne Information des Betroffenen dessen Daten an das Tumorzentrum melden können, wenn sie bei einer Gewebeuntersuchung einen bösartigen Tumor diagnostizieren. Dieser Weg wurde damit begründet, dass die behandelnden Ärzte im Krankenhaus oder in der Klinik einer erheblichen Arbeitsbelastung ausgesetzt seien und sie deshalb die Patienten aus Zeitgründen nicht bitten würden, in die Speicherung ihrer Daten einzuwilligen.

Ich habe empfohlen, die Einwilligungserklärung nicht in den Krankenhausaufnahmevertrag aufzunehmen. Eine Einwilligung muss stets bestimmt sein. Sie wäre aber nur dann bestimmt, wenn die betroffene Person bereits bei der Aufnahme weiß, dass ihre Daten für die Behandlung eines Tumors in diesem Register konkret verarbeitet werden sollen, und wenn sie darüber aufgeklärt worden ist. Dies wird aber nur ausnahmsweise zu diesem Zeitpunkt der Fall sein, so dass die Verbindung der Einwilligung mit dem Krankenhausaufnahmevertrag nicht sinnvoll ist. Ohnehin müsste es darüber hinaus möglich sein, dass ein Patient zwar den Krankenhausaufnahmevertrag unterschreibt, aber der Speicherung der Daten im klinischen Krebsregister widerspricht. Diese beiden Sachverhalte lassen sich daher kaum in eindeutiger Weise in einem Formular unterbringen.

Im Übrigen ist eine Aufklärung über eine medizinische Behandlung nach der Berufssordnung für die Ärztinnen und Ärzte in Mecklenburg-Vorpommern ohnehin erforder-

derlich (§ 8 BOÄ M-V). Im Rahmen dieser Aufklärung kann auch die Einwilligung eingeholt werden.

3.12.6 Novellierung des Landeskrankenhausgesetzes

Im Jahr 2001 hat der Landtag im Rahmen eines Gesetzes zur Neuregelung von Aufgaben im Öffentlichen Gesundheitsdienst auch das Landeskrankenhausgesetz (LKHG M-V) geändert. Meine Empfehlungen zum Gesetzentwurf wurden dabei überwiegend berücksichtigt.

Unter anderem regelt § 18 LKHG M-V das allgemeine Auskunftsrecht neu. Bislang galt das Auskunfts- und Akteneinsichtsrecht nur für den Patienten und nur für seine Daten, nicht jedoch für Daten von Angehörigen und sonstigen Dritten. Zu den Patientendaten gehören aber nach der Legaldefinition des Landeskrankenhausgesetzes auch solche von Angehörigen oder anderen Bezugspersonen sowie sonstigen Dritten, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden. An den § 18 wurde ein neuer Absatz 3 angefügt. Nunmehr haben die oben genannten Personengruppen ebenso wie der Patient ein Recht auf kostenfreie Auskunft zu den zu ihrer Person gespeicherten Daten, wenn der Auskunft schutzwürdige Belange des Patienten nicht entgegenstehen. Durch die Novellierung wurde zudem das von Artikel 12 der EG-Datenschutzrichtlinie (EG-DSRL) geforderte Auskunftsrecht in ein nationales Gesetz umgesetzt.

Des Weiteren wurde der Paragraph für die Datenverarbeitung im Auftrag (§ 21 LKHG M-V) neu geregelt. Die Neuregelung war nötig, weil in letzter Zeit die Tendenz zur Auslagerung von Aufgaben öffentlich-rechtlicher Stellen auch in Bereichen mit besonderer Geheimhaltungspflicht zu beobachten ist. Werden Patientendaten im Auftrag verarbeitet, also von einem Auftragnehmer außerhalb des Krankenhauses, sind insbesondere die Bestimmungen der EG-DSRL zu berücksichtigen. Personen außerhalb öffentlicher Stellen dürfen nach Art. 8 Abs. 3 dieser Richtlinie Daten für Zwecke der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten nur dann verarbeiten, wenn auch für sie Berufsgeheimnisse oder entsprechende Geheimhaltungspflichten gelten. Es war also zu klären, wie dies bei einer Datenverarbeitung im Auftrag realisiert werden kann.

Die Geheimhaltungsvorschrift des § 203 Strafgesetzbuch (StGB; ärztliche Schweigepflicht) kann grundsätzlich nicht unmittelbar auf Mitarbeiter eines Auftragnehmers angewendet werden. Diese Norm ist zwar auch auf die Tätigkeit eines ärztli-

chen Gehilfen anwendbar. Bei einem Auftragnehmer, der für ein Krankenhaus eine Serviceleistung erbringt, handelt es sich jedoch in der Regel um einen selbständigen Gewerbetreibenden, der rechtlich unabhängig von dem Krankenhaus ist und das wirtschaftliche Risiko selbst trägt. Daher fällt der Auftragnehmer nicht unter den Begriff des Gehilfen. Auch ist zweifelhaft, ob die Voraussetzungen der EG-DSRL erfüllt sind.

Auch auf das allgemeine Datengeheimnis gemäß § 5 Landesdatenschutzgesetz als eine von Art. 8 Abs. 3 der EG-Datenschutzrichtlinie geforderte entsprechende Geheimhaltungsvorschrift kann nicht zurückgegriffen werden. Das Strafmaß entspricht zwar dem der Geheimhaltungsvorschrift des § 203 StGB, aber das allgemeine Datengeheimnis ist anders als die Geheimhaltungsvorschrift nach § 203 StGB nicht mit dem für den Schutz von Patientendaten notwendigen Zeugnisverweigerungsrecht verbunden.

Es ist aber nicht realistisch, bei Patientendaten die Auftragsdatenverarbeitung außerhalb des Krankenhauses generell zu unterbinden. Daher war zu prüfen, ob im Gesundheitsbereich eine Datenverarbeitung im Auftrag unter anderen Voraussetzungen zulässig ist. Art. 8 Abs. 4 der EG-DSRL bestimmt, dass Mitgliedstaaten aus Gründen eines wichtigen öffentlichen Interesses im Wege einer nationalen Rechtsvorschrift Ausnahmen von dem Verarbeitungsverbot vorsehen dürfen. Allerdings werden dann angemessene Garantien verlangt. § 21 LKHG M-V kann als eine solche nationale Ausnahme gesehen werden. Gemäß § 21 ist eine Datenverarbeitung beispielsweise dann im Auftrag zulässig, wenn sie erheblich kostengünstiger als im Krankenhaus ist oder wenn das Krankenhaus seinen Betrieb einstellt. Bevor ein Krankenhaus einen solchen Auftrag erteilt, muss es jedoch prüfen und dokumentieren, ob und welche gesetzliche Voraussetzung dafür vorliegt.

Darüber hinaus war es nötig, eine Vorschrift in das neue Landeskrankenhausgesetz aufzunehmen, nach der regelmäßig zu prüfen ist, ob die Auftragsdatenverarbeitung mit verschlüsselten oder pseudonymisierten Daten durchgeführt werden kann. Damit könnten Patientendaten wirkungsvoll gegen nicht erforderliche oder unberechtigte Kenntnisnahme geschützt werden. Der Gesetzgeber folgte dieser Anregung und nahm in § 21 eine entsprechende Regelung auf.

Im novellierten Gesetz sind weitere, besondere Schutzmaßnahmen für die Verarbeitung von Patientendaten im Auftrag normiert. So hat das Krankenhaus den Auftragnehmer sorgfältig auszuwählen. Die Einzelheiten des Auftrags und die vom Auftragnehmer zu treffenden technischen und organisatorischen Sicherungsmaßnahmen sind schriftlich zu vereinbaren. Der Landesbeauftragte für den Datenschutz ist über

das Auftragsverhältnis nicht nur zu informieren, sondern er muss eine Abschrift der Vereinbarung erhalten. Eine Verschärfung gegenüber den Regelungen zur Auftragsverarbeitung im Landesdatenschutzgesetz enthält § 21 Abs. 5 LKHG M-V. Hier ist normiert, dass der Auftragnehmer die Datenverarbeitung nicht ohne Zustimmung des Krankenhauses auf Dritte übertragen darf und dass dann auch dieselben Schutzvorschriften wie beim ursprünglichen Auftragnehmer zu beachten sind.

3.13 Personalwesen

3.13.1 Personaldaten im Datennetz

Ein Beschäftigter einer Polizeibehörde teilte mir mit, dass Daten aus einem Personalvorgang über ihn für alle Mitarbeiter seiner Dienststelle in dem dort genutzten Datenverarbeitungssystem lesbar seien. Darüber hinaus könnten auch Mitarbeiter in anderen Polizeidienststellen, die das System berechtigt nutzen können, seine Daten zur Kenntnis nehmen.

Daraufhin habe ich die Verarbeitung der Daten in der Polizeibehörde kontrolliert. Der Behördenleiter bestätigte bei der Kontrolle, dass Personaldaten vorübergehend in einem Bereich des Dienststellenservers gespeichert waren, der nicht gegen die Kenntnisnahme durch andere Beschäftigte geschützt war.

Das Konzept der Datenhaltung sieht vor, dass für jeden berechtigten Nutzer auch ein persönliches Verzeichnis von Dateien für Zwecke der Bürokommunikation auf dem Server eingerichtet wird. Schreib- und Leserechte für Dateien dieses Verzeichnisses hat nur der Inhaber dieses Verzeichnisses. Jedoch kann er seine Rechte auch auf weitere Nutzer oder auf alle übertragen.

Im konkreten Fall hatten Personalsachbearbeiter Schriftstücke zu Personalvorgängen in ihrem persönlichen Verzeichnis gespeichert. Einem Vertreter des Sachbearbeiters war es dadurch nicht mehr möglich, die Vorgänge weiter zu bearbeiten. Deshalb beauftragte der Vorgesetzte eine Personalsachbearbeiterin, ein Verzeichnis für Personalvorgänge anzulegen, das von den anderen mit der Verarbeitung dieser Daten betrauten Mitarbeitern genutzt werden kann. Die Sachbearbeiterin führte diesen Auftrag aus und öffnete den Zugriff auf die entsprechenden Dateien. Später stellte sich heraus, dass neben den Personalsachbearbeitern auch weitere Nutzer des Datenverarbeitungssystems der Dienststelle Zugriff auf das Verzeichnis hatten. Sogar aus anderen Polizeidienststellen war der Zugriff möglich, wenn Nutzer in der Lage waren, über das Weitverkehrsnetz eine Verbindung zu diesem Dienststellenserver herzustellen.

Bei der Kontrolle war nicht mehr festzustellen, ob und welche Nutzer tatsächlich auf die Personaldaten in dem neu eingerichteten Verzeichnis zugegriffen hatten. Die Zugriffe auf Daten in solchen Bürokommunikationsanwendungen wurden nicht revisionsicher protokolliert (siehe Punkt 3.3.1). Auf dem Dienststellenserver wurde lediglich das so genannte Journal gespeichert, das die Bürokommunikationsaktivitäten

jedes Nutzers widerspiegelt. Weil die jeweiligen Nutzer mit Hilfe ihrer persönlichen Chipkarte ihre Daten in dem Journal jederzeit teilweise oder vollständig löschen konnten, waren die Aktivitäten nicht mehr nachvollziehbar.

Gegenüber dem Innenminister habe ich die unzureichenden technischen und organisatorischen Maßnahmen zur Datensicherheit beanstandet. Nach dem Landesbeamtenengesetz (LBG M-V) dürfen nur Beschäftigte Zugang zur Personalakte haben, die im Rahmen der Personalverwaltung beauftragt sind, Personalangelegenheiten zu bearbeiten. Der Zugriff auf die Daten darf auch nur in dem Umfang erfolgen, soweit er erforderlich ist (§ 100 Abs. 3 LBG M-V). Diese Vorschrift gilt auch für die automatisierte Datenverarbeitung. Ich habe darauf hingewiesen, dass sich das Bürokommunikationssystem grundsätzlich nicht zur Personaldatenverarbeitung eignet, weil es nur unzureichend gegen unberechtigte Zugriffe abgesichert ist. Darüber hinaus habe ich empfohlen, künftig auch im Polizeibereich das durch Kabinettsbeschluss als Landesstandard festgelegte Elektronische Personal-, Organisations- und Stellenverwaltungssystem (EPOS) einzusetzen.

Der Innenminister hat meine Empfehlungen und Hinweise umgesetzt und landesweit Maßnahmen zum Schutz von Personaldaten in den Polizeidienststellen getroffen, die das kontrollierte Datenverarbeitungssystem einsetzen. Er hat die Dienststellen außerdem aufgefordert, auf der Grundlage des IT-Sicherheitskonzeptes und der entsprechenden Anwenderrichtlinie regelmäßige Schulungen und Belehrungen durchzuführen. Nunmehr wird der Einsatz von EPOS im gesamten Bereich der Polizei vorbereitet.

Den Mitarbeiter der Polizeibehörde, der mich über den Umgang mit seinen Daten informiert hatte, habe ich über das Ergebnis meiner Kontrolle informiert.

3.13.2 Aktennotiz zur Vorbereitung eines Gesprächs

Mir ist eine Aktennotiz zur Kenntnis gegeben worden, die detailliert das dienstliche Verhalten eines Arztes sowie seine persönlichen Lebensumstände beschreibt. Der Arzt war als leitender Notarzt in einem Landkreis eingesetzt. Als ich von der Notiz erfuhr, waren bereits Einzelheiten daraus in der Öffentlichkeit bekannt gemacht worden. Um den Vorgang datenschutzrechtlich bewerten zu können, habe ich den Umgang mit den für diesen Fall relevanten Daten in der Verwaltung des Landkreises kontrolliert.

Ziel der Kontrolle war es zu klären, wer die Notiz zu welchem Zweck und auf welcher Rechtsgrundlage angefertigt hatte, ob die Daten noch gespeichert sind und ob

sie genutzt werden. Außerdem war zu prüfen, ob die technischen und organisatorischen Maßnahmen bei der Verarbeitung personenbezogener Daten angemessen sind und auf welche Weise die Daten in die Öffentlichkeit und damit Dritten zur Kenntnis gelangen konnten.

Die Aktennotiz hatte eine Mitarbeiterin der Rettungsleitstelle des Landkreises angefertigt. Sie sollte nach Aussage der verantwortlichen Mitarbeiter der Landkreisverwaltung als Grundlage für ein Gespräch mit dem Arzt dienen. Die Notiz war nur zur internen Verwendung bestimmt und sei nicht an Dritte weitergegeben worden. Die Mitarbeiter der Landkreisverwaltung konnten sich nicht erklären, wie die Notiz an die Öffentlichkeit gelangt war. Sie sei im Datenverarbeitungssystem inzwischen gelöscht und der Ausdruck nach dem Gespräch vernichtet worden. Der Betroffene ist über den Inhalt der Notiz jedoch nicht informiert worden.

Unter Mitwirkung des IT-Verantwortlichen der Landkreisverwaltung wurden die gespeicherten Dateien sowie die Zugriffsrechte und die weiteren Maßnahmen zum Schutz der Daten kontrolliert. Es ergaben sich keine Hinweise darauf, dass sich Dritte die Daten unberechtigt verschafft hatten. Eine Auswertung der Protokolle des Servers, über den E-Mails gesendet und empfangen werden, ergab jedoch, dass die Aktennotiz von der Mitarbeiterin, die sie erstellt hatte, an den Arbeitgeber des Notarztes versandt worden ist. Nachdem dieser Sachverhalt bekannt geworden war, bestätigte die Mitarbeiterin, die Notiz als E-Mail dorthin versandt zu haben.

Das Rettungswesen ist eine öffentliche Aufgabe, für die der Landkreis zuständig ist. Der Arbeitgeber des Arztes ist aber eine nichtöffentliche Stelle. Zwischen diesen Stellen dürfen Daten nur übermittelt werden, wenn eine Rechtsvorschrift dies vorsieht oder der Betroffene eingewilligt hat. Für die Verarbeitung der Daten über den Notarzt sowie die Übermittlung der Notiz an den Arbeitgeber existierte jedoch weder eine Rechtsgrundlage noch eine Einwilligung. Deshalb waren sie unzulässig und stellen einen Verstoß gegen datenschutzrechtliche Vorschriften dar. Dies habe ich gegenüber dem Landrat des Landkreises beanstandet und die zuständige oberste Landesbehörde informiert.

Personenbezogene Daten dürfen nur genutzt und verarbeitet werden, wenn und soweit es zur Aufgabenerfüllung der nutzenden beziehungsweise verarbeitenden Stelle erforderlich ist. Dies war hier nach dem Rettungsdienstgesetz von Mecklenburg-Vorpommern zu beurteilen. Danach können beispielsweise Daten verarbeitet werden, wenn es um Dienstpflichtverletzungen geht. Aus der Notiz ging aber nicht eindeutig hervor, ob dem Arzt Dienstpflichtverletzungen vorgeworfen wurden. Die Notiz be-

schrieb lediglich persönliche Lebensumstände des Notarztes und erweckte den Anschein, dass er ausgeforscht wurde. So wurde beispielsweise notiert, dass der Arzt eine Freundin habe, die ebenfalls Notärztin sei und die er an einem bestimmten Tag anrufen habe. Bei dieser Feststellung fehlt es an einer erkennbaren dienstlichen Relevanz.

Notizen, die zur Vorbereitung von Gesprächen dienen, dürfen nur solche Daten enthalten, die dienstrechtlich relevant sind. Ich habe empfohlen, betreffende Personen vor einem Gespräch darüber zu informieren, welche Daten über sie gespeichert sind. Außerdem sind Auswertungsverfahren für Protokolldaten und Speicherfristen festzulegen. Sensible Daten sollten bei ihrer Speicherung und vor einer Übermittlung mit einem sicheren kryptographischen Verfahren verschlüsselt werden. Die Mitarbeiter des Landkreises sollten in einer Dienstanweisung oder Schulung informiert werden, unter welchen Voraussetzungen sie eine E-Mail versenden dürfen und welche Schutzmaßnahmen einzuhalten sind.

Der Landrat ist meinen Empfehlungen gefolgt und hat meine Hinweise umgesetzt. Eine Dienstanweisung wurde erarbeitet. Den betroffenen Notarzt habe ich über meine datenschutzrechtliche Bewertung informiert.

3.13.3 Elektronische Aufzeichnung von Personalgesprächen?

Der Personalrat einer Stadtverwaltung hat mich darüber informiert, dass ein Vorgesetzter ein Personalgespräch mit einer Mitarbeiterin ohne deren Wissen aufgezeichnet hat. Der Vorgesetzte wollte auf der Grundlage dieser Aufzeichnung einen Aktenvermerk anfertigen und hat die Kasette zu diesem Zweck aufbewahrt. Der Sachverhalt ist datenschutzrechtlich wie folgt zu bewerten:

Die Art einer Datenerhebung muss zum angestrebten Zweck in einem angemessenen Verhältnis stehen. Im konkreten Fall hätte der Aktenvermerk ebenso auf der Basis von handschriftlichen Notizen des Vorgesetzten angefertigt werden können. Sollen Personalgespräche dennoch elektronisch aufgezeichnet werden, ist dafür das Einverständnis der betroffenen Person erforderlich, da diese bei der elektronischen Aufzeichnung regelmäßig unbewusst mehr Daten preisgibt, als dies für den angestrebten Zweck erforderlich ist.

Ich habe der Stadtverwaltung empfohlen, die aufgezeichneten Daten zu löschen, weil die Einwilligung der betroffenen Mitarbeiterin nicht vorlag und die elektronische Aufzeichnung deshalb nicht rechtmäßig war. Sofern künftig dennoch erwogen wird,

ein Personalgespräch elektronisch aufzuzeichnen, muss die betroffene Person vorher einwilligen und in geeigneter Art und Weise über den Zweck der Erhebung sowie die Art und den Umfang der Verarbeitung und Nutzung der Daten aufgeklärt werden.

Die Stadtverwaltung informierte mich, dass die Daten gelöscht wurden und meine Empfehlungen künftig umgesetzt werden.

3.13.4 Keine Offenbarungspflicht bei Fragen nach bereits getilgten Straftaten

Vor einer Einstellung in den öffentlichen Dienst oder einer Berufung in das Beamtenverhältnis haben Betroffene regelmäßig auch eine Erklärung über von ihnen begangene Straftaten abzugeben. In dem vom Innenministerium unseres Landes konzipierten Vordruck wird der Betroffene darauf hingewiesen, dass er gemäß § 53 Abs. 2 Bundeszentralregistergesetz (BZRG) verpflichtet sei, alle Verurteilungen anzugeben, auch wenn diese nicht in ein Führungszeugnis aufzunehmen oder bereits getilgt worden sind. Diese Aussage steht teilweise im Widerspruch zur geltenden Rechtslage.

Nach § 51 Abs. 1 BZRG dürfen die Tat und die Verurteilung dem Betroffenen im Rechtsverkehr nicht mehr vorgehalten und nicht zu seinem Nachteil verwertet werden, wenn die Eintragung über eine Verurteilung im Bundeszentralregister bereits getilgt worden oder zu tilgen ist. Als Folge dieses Vorhalte- und Verwertungsverbotes darf sich der Betroffene ab diesem Zeitpunkt gemäß § 53 Abs. 1 Nr. 2 BZRG als unbestraft bezeichnen. Die Tilgungsvorschriften, das Vorhalte- und Verwertungsverbot und das damit verbundene Verschweigerecht des Betroffenen sollen ihm die Resozialisierung und den Einstieg in das berufliche Leben erleichtern. Diese Rechte des Betroffenen gelten auch im öffentlichen Dienst.

Eine Ausnahme vom Verschweigerecht sieht § 53 Abs. 2 BZRG lediglich in den Fällen vor, in denen die Verurteilungen nicht in das Führungszeugnis oder nur in ein Führungszeugnis nach § 32 Abs. 3 und 4 BZRG aufzunehmen sind und der Betroffene über das unbeschränkte Auskunftsrecht der Gerichte und Behörden belehrt worden ist. Insoweit ist der Vordruck des Innenministeriums zutreffend. Für zu tilgende oder bereits getilgte Verurteilungen gilt diese Ausnahme jedoch nicht. § 53 Abs. 2 BZRG schränkt das Verschweigerecht nur in den Fällen des § 53 Abs. 1 Nr. 1 BZRG ein, das heißt gerade nicht bei getilgten oder tilgungsreifen Verurteilungen. Eine Pflicht des Betroffenen, Auskunft über getilgte Straftaten zu geben, besteht nach § 53 Abs. 1 Nr. 2 BZRG somit nicht. Dies gilt ungeachtet der Tatsache, dass nach § 52 Abs. 1 Nr. 4 BZRG bei Einstellungen in den öffentlichen Dienst eine Ausnah-

me vom Verwertungsverbot nach § 51 Abs. 1 BZRG vorliegt. Diese Ausnahme soll lediglich dazu dienen, dass die Stelle Informationen zu Verurteilungen, die ihr rechtmäßig vorliegen, in engen Grenzen trotz des Verwertungsverbotes noch nutzen darf. Zur Datenerhebung beim Betroffenen oder bei Dritten wird sie dadurch nicht ermächtigt.

Mithin werden die Unterzeichner der Formulare durch die falsche Belehrung über die in diesen Fällen angeblich bestehende Auskunftspflicht in ihrem Verschweigerrecht aus § 53 BZRG und damit in ihrem Grundrecht auf informationelle Selbstbestimmung erheblich beeinträchtigt.

Ich habe dem Innenministerium deshalb empfohlen, die im Vordruck genannte Auskunftspflicht für bereits getilgte Straftaten zu streichen. Eine Antwort lag bis Redaktionsschluss nicht vor.

3.13.5 Einsicht in Personalunterlagen für potentielle Käufer

Ich erhielt einen Hinweis, dass den möglichen Käufern des Flughafens Parchim-Mecklenburg, der zu diesem Zeitpunkt ein öffentlich-rechtliches Unternehmen war, Einsicht in Personalunterlagen der dort beschäftigten Mitarbeiter gewährt würde.

Das Wirtschaftsministerium hatte den potentiellen Käufern einen Raum in seinem Gebäude zur Verfügung gestellt, in dem diese die relevanten Unterlagen des Unternehmens einsehen konnten. Darunter befanden sich auch Akten über abgeschlossene Rechtsstreitigkeiten, die gegen Mitarbeiter des Flughafens oder von diesen gegen den Flughafen geführt worden waren. Unter anderem enthielten die Ordner umfangreichen Schriftwechsel zu arbeitsrechtlichen Streitigkeiten sowie Korrespondenz zu einem rechtskräftigen Strafbefehl gegen einen Mitarbeiter.

Nachdem ich auf die fehlende Rechtsgrundlage für diese Datenübermittlung an Dritte hingewiesen hatte, wurden die Unterlagen unverzüglich aus dem Raum entfernt. Sie sollten den möglichen Käufern erst wieder zur Verfügung gestellt werden, wenn die Sach- und Rechtslage geklärt war. In diesem Zusammenhang machte der Geschäftsführer des Flughafens deutlich, dass mit ernsthaften Bemühungen um den Erwerb der Gesellschaft nur zu rechnen sei, wenn potentielle Investoren einen umfassenden Einblick in das Unternehmen erhalten. Nur dann könnten diese ihr eigenes wirtschaftliches Risiko abschätzen.

Beim Umgang mit Personaldaten ist § 31 Landesdatenschutzgesetz von Mecklenburg-Vorpommern zu beachten. Danach dürfen öffentliche Stellen mit Daten ihrer Beschäftigten nur umgehen, wenn es im Zusammenhang mit Dienst- oder Arbeitsverhältnissen oder zur Durchführung innerdienstlicher organisatorischer, sozialer und personeller Maßnahmen erforderlich ist oder wenn eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung es vorsehen. Im Rahmen von Verkaufsverhandlungen können Personalinformationen wie Anzahl der Mitarbeiter und deren Alter, Beruf und Qualifikation tatsächlich von Bedeutung sein. Personaldaten über Rechtsstreitigkeiten waren im vorliegenden Fall jedoch nicht erforderlich. Dieses habe ich dem Geschäftsführer des Flughafens mitgeteilt und darauf hingewiesen, beim Umgang mit Personaldaten künftig entsprechend den gesetzlichen Vorschriften zu verfahren.

3.14 Bildung, Kultur, Wissenschaft und Forschung

3.14.1 Sicherheit für die personenbezogenen Daten im Bildungsministerium

Mitte des Jahres 2001 wurde der Internetzugang des Bildungsministeriums kontrolliert. Im Unterschied zu den anderen Ministerien des Landes nutzt das Bildungsministerium nicht die zentrale Firewall der DVZ M-V GmbH (siehe Punkt 3.18.1), sondern betreibt eine eigene Firewall. Deshalb war ein Ziel dieser Kontrolle, die Sicherheitsniveaus dieser beiden Lösungen zu vergleichen und festzustellen, wie sie sich ergänzen können.

Zur IT-Politik im Bildungsministerium gehört, sich nach außen möglichst offen und kommunikativ zu zeigen und dabei ganz bewusst auf moderne elektronische Kommunikationsmöglichkeiten zu setzen. Darüber hinaus besteht in vielen Bereichen des Ministeriums selbst ein hoher Informationsbedarf, der häufig nur mit Hilfe des Internet in angemessener Zeit befriedigt werden kann. Ein weiteres Motiv für die Internetnutzung ist die regelmäßige Kommunikation mit den wissenschaftlichen Einrichtungen Mecklenburg-Vorpommerns. Deshalb wurde festgelegt, allen Nutzern von PC-Arbeitsplätzen weitgehend uneingeschränkter Zugriff auf das Internet zu ermöglichen. An jedem Bildschirm-Arbeitsplatz kann auch E-Mail direkt versandt und empfangen werden.

Um bewerten zu können, welche Datenschutzmaßnahmen im Einzelnen angemessen sind, habe ich mich zunächst über den konkreten Kommunikationsbedarf des Ministeriums informiert. Elektronische Kommunikationsbeziehungen bestehen demnach vor allem zu den Hochschulen des Landes sowie zu den Schulämtern und den Schulen. In den Schulämtern und im Ministerium kommt auch die Personalverwaltungssoftware PERSYS zum Einsatz. Der Kommunikationsbedarf zu anderen Ressorts ist demgegenüber gering. Lediglich das vom Finanzministerium betriebene Verfahren PROFiskal (siehe Punkt 3.10.4) wird in größerem Umfang genutzt.

Die von der IT-Abteilung des Bildungsministeriums betriebene Firewall erwies sich als dem Stand der Technik entsprechend eingerichtet und sorgfältig administriert. Dies trifft auch auf die flankierenden technischen Maßnahmen zu, die die Arbeitsplatzrechner vor Manipulationen schützen.

Die Firewall enthält neben Paket-Filtern auch ein Application Gateway und beherrscht die Adressumsetzung (NAT). Zentrale Server wurden in einem Bereich platziert, der sowohl zum Internet als auch zum lokalen Netz hin von der Firewall geschützt ist,

einer so genannten Demilitarisierten Zone (DMZ). Ein automatischer Virenschanner prüft elektronische Post und andere übertragene Sendungen auf gefährliche Inhalte. Überdies ist ein virtuelles privates Netz (VPN) eingerichtet, welches die Firewall des Bildungsministeriums mit den Firewalls der Schulämter und der Schulen kryptographisch gesichert miteinander verbindet.

Dennoch habe ich dem Ministerium noch folgende technische Verbesserungen empfohlen:

- Die Administrationsaktivitäten sollten nicht wie bisher manuell, sondern automatisiert protokolliert werden.
- An der Firewall werden bislang bestimmte Nachrichten aufgezeichnet, die von den Arbeitsplatzrechnern regelmäßig in das lokale Netz gesendet werden. Die Firewall sollte diese Sendungen nicht mehr protokollieren, da sie nicht sicherheitsrelevant sind.
- Externe Kommunikationspartner sollten mit dem Bildungsministerium verschlüsselt kommunizieren können.
- Schließlich bedürfen einige Räume mit zentraler Informationstechnik einer besseren Zugangssicherung. Es sollte auch dafür gesorgt werden, dass dort weniger brennbare Materialien lagern.

Im Gegensatz zum guten Prüfungsergebnis im technischen Bereich waren die organisatorischen Datenschutzmaßnahmen nicht ausreichend. Vor allem sind die bereits getroffenen technischen Maßnahmen zum Datenschutz nur unzureichend dokumentiert worden. Die hierfür erforderlichen Unterlagen wie Datenschutz- und IT-Sicherheitskonzept, Revisionsunterlagen, Sicherheits-Policy sind nicht vorhanden. Deshalb können die eigenen Mitarbeiter und auch externe Prüfer die Bedrohungen und den daraus resultierenden Schutzbedarf für die verarbeiteten Daten und die einzelnen Anwendungen nur wesentlich schwerer objektiv bewerten. Ob die gewählten Sicherheitsmaßnahmen tatsächlich ausreichend und angemessen sind, ist ohne diese Unterlagen nur mit erheblichem zusätzlichem Prüfaufwand bewertbar.

Zu den Schwachstellen im organisatorischen Bereich habe ich unter anderem folgende Veränderungen empfohlen:

- Es sind revisionsfähige Datenschutz- und IT-Sicherheitskonzepte zu erstellen, mit denen der Schutzbedarf der einzelnen Anwendungen, die Bedrohungen, die kor-

respondierenden IT-Sicherheitsmaßnahmen und die verbleibenden Restrisiken nachvollzogen werden können. Arbeitsplätze, auf denen personenbezogene Daten mit hohem Schutzbedarf verarbeitet werden, sind in den Konzepten besonders zu berücksichtigen. Hierzu gehören PROFiskal- und PERSYS-Arbeitsplätze.

- Im Geschäftsbereich des Bildungsministeriums sollten regelmäßig Revisionen der IT-Sicherheit durchgeführt werden, insbesondere im Ministerium selbst und in den vier Schulämtern. Grundsätzlich sollte ein Mitarbeiter des Ministeriums als weisungsunabhängiger IT-Sicherheitsbeauftragter diese Aufgabe wahrnehmen. Es erscheint sinnvoll, auch andere Ressorts in diese Überlegungen einzubeziehen, zum Beispiel über die Firewall-Revisionsgruppe (siehe Punkt 3.18.1).
- Die Regelungen des Bildungsministeriums zur Internetnutzung sind bereits mehrere Jahre alt und spiegeln nicht die neuen Möglichkeiten von Internet und E-Mail wider. Das hausinterne Regelwerk ist dem Entwicklungsstand anzupassen. Dabei ist auch darauf zu achten, dass dienstliche und private E-Mail voneinander getrennt wird, um das Post- und Fernmeldegeheimnis der Bediensteten zu respektieren (siehe Punkt 3.17.5).
- Das Bildungsministerium hat ein Unternehmen mit der Fernwartung von Netzwerken in den Schulämtern des Landes und im eigenen Hause beauftragt. Dabei wurde unter anderem versäumt, Vereinbarungen zum technischen Datenschutz, zur Verpflichtung der Mitarbeiter auf das Datengeheimnis und zu Unterauftragsverhältnissen zu treffen. Dies ist nachzuholen.

Bis zum Redaktionsschluss hat das Bildungsministerium auf diese Bewertungen und Empfehlungen noch nicht reagiert. Wenn aber die organisatorischen Mängel behoben sind, dann gewährleistet die ministeriumseigene Firewall ein Schutzniveau, welches der zentralen Firewall der DVZ M-V GmbH in nichts nachsteht. Unter diesen Voraussetzungen halte ich es für sinnvoll, beide Firewalls hintereinander zu schalten. So entstünde eine gestaffelte Firewall, die sich zur Kopplung von Netzen mit hohem Schutzbedarf eignet. Die Datenschutzbeauftragten des Bundes und der Länder haben diese Lösung in der Orientierungshilfe „Internet“ ausdrücklich empfohlen (siehe Vierter Tätigkeitsbericht, Punkte 3.16.4 und 4).

3.14.2 Datenübermittlung bei Fernleihen

Ein Nutzer einer Hochschulbibliothek beschwerte sich bei mir darüber, dass bei der Fernleihe von Literatur seine personenbezogenen Daten elektronisch an die ausleihende Bibliothek übermittelt werden. So könnten Dritte erfahren, mit welcher wissenschaftlichen Fragestellung er sich zurzeit befasse.

Die elektronische Übermittlung über das Internet und die Speicherung der Daten auf einem Server, den mehrere Bibliotheken gemeinsam zur organisatorischen Abwicklung der Fernleihe nutzen, eröffnen tatsächlich umfangreiche Auswertungsmöglichkeiten. Deshalb habe ich mit Mitarbeitern der Hochschulbibliothek über die datenschutzrechtliche Seite der Fernleihe beraten.

Im Ergebnis wurde folgende Lösung gefunden: Nutzer, die nicht wünschen, dass ihre personenbezogenen Daten elektronisch an die ausleihende Bibliothek übermittelt werden, können ihre Bestellung über die konventionelle Fernleihe (keine elektronische Übermittlung) oder elektronisch durch das Bibliothekspersonal abwickeln lassen. Im zweiten Fall werden nur Daten der bestellenden Bibliothek und die Benutzernummer elektronisch übermittelt. Aus dieser Nummer kann die bestellende Bibliothek den Nutzer dann wieder identifizieren.

Bei der Beratung zur Übermittlung der Daten über das Internet in eine zentrale Datenbank habe ich festgestellt, dass nicht alle Sicherheitsvorkehrungen gegen Angriffe von außen dem Stand der Technik entsprechen. Die sich schnell entwickelnden technischen Möglichkeiten liefern nicht nur Werkzeuge und Verfahren zum besseren Schutz der Daten, sondern eröffnen auch neue Angriffsszenarien. Vorhandene Sicherheitsmaßnahmen sind von der Daten verarbeitenden Stelle daher regelmäßig mit dem Ziel zu überprüfen, ob sie den Anforderungen noch genügen. Die Software der Bibliothek wird schon etliche Jahre genutzt und entspricht nicht mehr im vollen Umfang dem Stand der Technik. Ich habe deshalb entsprechende Maßnahmen empfohlen. Zurzeit wird ein neues Bibliothekssystem entwickelt, das in naher Zukunft eingesetzt werden soll. Mit diesem System wird ein höheres Sicherheitsniveau erreicht werden.

3.14.3 Datenschutzgerechte Nutzung des Archivgutes

Zur datenschutzgerechten Nutzung von personenbezogenem Archivgut gab es im Berichtszeitraum mehrere Anfragen. Ein Bürger hat mir beispielsweise mitgeteilt, dass

er beabsichtige, eine Informationssammlung über bedeutende Persönlichkeiten Mecklenburg-Vorpommerns zu erarbeiten. Er wollte wissen, welche datenschutzrechtlichen Bestimmungen zu beachten sind.

Datenschutzrechtlich unbedenklich ist es, wenn zu diesem Zweck Unterlagen genutzt werden, die bereits veröffentlicht wurden oder die allgemein zugänglichen Quellen entnommen werden können. Anders verhält es sich jedoch, wenn Material aus dem Archiv genutzt werden soll, das bisher noch nicht veröffentlicht worden ist. In diesem Fall sind die Bestimmungen des Landesarchivgesetzes (LArchivG M-V), insbesondere § 9, zu beachten. Danach kann jeder, der ein berechtigtes Interesse glaubhaft macht, das Archivgut nutzen. Von einem berechtigten Interesse kann zum Beispiel ausgegangen werden, wenn die Unterlagen zu amtlichen oder wissenschaftlichen Zwecken oder zur Wahrung berechtigter persönlicher Belange des Nutzers verwendet werden sollen. Das Archiv hat in diesem Zusammenhang jedoch zu prüfen, ob einer der im Landesarchivgesetz normierten Versagungsgründe vorliegt (§ 9 Abs. 2 LArchivG). Unter anderem muss es einen Antrag auf Nutzung des Archivgutes ablehnen, wenn Geheimhaltungspflichten entgegenstehen. So unterliegen beispielsweise Angaben über den Gesundheitszustand eines Menschen, die ein Arzt dokumentiert hat, der ärztlichen Schweigepflicht. Die ärztliche Schweigepflicht gehört zu den Berufspflichten jedes Arztes, deren Verletzung gemäß § 203 Strafgesetzbuch unter Strafe gestellt ist. Nur wenn eine Verletzung der Geheimhaltungspflicht nicht zu befürchten ist, können die Unterlagen genutzt werden.

Darüber hinaus sind auch entsprechende Schutzfristen zu beachten. Danach darf personenbezogenes Archivgut erst zehn Jahre nach dem Tod des Betroffenen oder, wenn das Todesdatum nicht bekannt ist, 90 Jahre nach dessen Geburt genutzt werden. Ist beides nicht mehr feststellbar, ist eine Nutzung erst 60 Jahre nach der Entstehung der Unterlagen möglich. Die Schutzfristen können verkürzt werden, wenn Hinterbliebene (Ehegatten oder Kinder) in die Nutzung der Daten einwilligen.

Ich habe die Bürger, die sich an mich gewandt hatten, über die Rechtslage informiert.

3.14.4 Evaluation an den Hochschulen

Im Rahmen von Lehr-Evaluationen werden unter anderem Studenten zur Qualität einzelner Lehrveranstaltungen an Universitäten und Fachhochschulen unseres Landes befragt. Sie sollen beispielsweise den Titel von Veranstaltungen angeben, die sie als besonders gut beziehungsweise als wenig oder nicht gelungen beurteilen, und dazu die Namen der jeweiligen Hochschullehrer nennen.

Dieses Verfahren greift in das Recht auf informationelle Selbstbestimmung der Hochschullehrer ein, denn um die Lehrqualität beurteilen zu können, werden personenbezogene Daten der Lehrer bei den Studenten erhoben und anschließend durch entsprechende Stellen der Hochschule verarbeitet. Daher bedürfen Lehr-Evaluationen einer normklaren gesetzlichen Grundlage oder der Einwilligung der betroffenen Person.

Das Landeshochschulgesetz enthält bisher keine gesetzlichen Regelungen für den Umgang mit personenbezogenen Daten bei Lehr-Evaluationen. Allerdings, und darauf habe ich das Ministerium für Bildung, Wissenschaft und Kultur hingewiesen, wäre es zulässig, wenn die Hochschulen in einer Satzung die Art und Weise der Evaluation und den damit verbundenen Umgang mit personenbezogenen Daten normieren. Dieses wäre auch von der bestehenden Rechtslage gedeckt. Das Ministerium hat den Hochschulen daraufhin empfohlen, umgehend eine Satzung zur Evaluation zu erlassen.

Im Zuge der Novellierung des Landeshochschulgesetzes wird nunmehr, voraussichtlich in § 32, die Evaluation der Lehre geregelt. Es wird aber, anders als in einigen anderen Bundesländern, keine ausdrückliche Vorschrift zum Umgang mit personenbezogenen Daten für diesen Zweck aufgenommen, sondern es wird normiert werden, dass die Hochschulen dies in einer Ordnung selbst regeln sollen.

3.15 Wirtschaft und Gewerbe

3.15.1 Einwilligungserklärung bei der Beantragung von Mitteln zur Ausbildungsplatzförderung

Eine Petentin schilderte mir folgenden Sachverhalt und hat mich gebeten, diesen datenschutzrechtlich zu bewerten:

Unternehmen aus Mecklenburg-Vorpommern können beim Wirtschaftsministerium Zuwendungen für betriebliche Berufsausbildungsverhältnisse beantragen. Zu den Antragsunterlagen gehört auch eine Einwilligungserklärung, in der der antragstellende Betrieb sich damit einverstanden erklärt, dass das Ministerium die in diesem Zusammenhang erhobenen personenbezogenen Daten an insgesamt zwölf Stellen übermittelt. In der Erklärung wird lediglich ausgeführt, dass dies aufgrund gesetzlicher Mitteilungspflichten erforderlich sei. Um welche Mitteilungspflichten es sich dabei handelt, wurde jedoch nicht dargelegt.

Eine solche Einwilligungserklärung entspricht nicht den datenschutzrechtlichen Bestimmungen. Deshalb habe ich dem Wirtschaftsministerium empfohlen, den Antragstellern in der Erklärung mitzuteilen, zu welchem Zweck die Daten bei den einzelnen Empfängern erforderlich sind. Darüber hinaus sind sie über die Art und den Umfang der Verarbeitung und Nutzung aufzuklären. Sofern in den Anträgen auch Daten der Inhaber eines geförderten Ausbildungsplatzes erfragt werden, sollten die Betroffenen ebenfalls in geeigneter Weise über den Zweck der Erhebung, die Art und den Umfang der Verarbeitung und Nutzung sowie über die Empfänger beabsichtigter Übermittlungen informiert werden. Des Weiteren habe ich gebeten zu prüfen, ob es tatsächlich erforderlich ist, die Daten an zwölf Stellen zu übermitteln.

Das Wirtschaftsministerium hat die Einwilligungserklärung überarbeitet. Dabei hat es zwar die Anzahl der Daten empfangenden Stellen auf immerhin vier reduziert, inhaltlich aber kaum etwas geändert. Insbesondere war nicht vorgesehen, die Auszubildenden über die Datenübermittlung zu informieren.

Ab September 2000 ist der datenschutzrechtliche Teil des Förderprogrammes mit dem ebenfalls beteiligten Ministerium für Arbeit und Bau weiter besprochen worden. Es konnten dann auch Verbesserungen bei der Aufklärung der Betroffenen über die Datenverarbeitung und -nutzung erreicht werden. Künftig erhalten sowohl der Ausbildungsbetrieb als auch der Auszubildende die erforderlichen Informationen über das Verfahren. Die Auszubildenden erfahren vor der Unterzeichnung des Aus-

bildungsvertrages, dass es sich um einen Ausbildungsplatz handelt, der vom Land, dem Bund und der Europäischen Union gefördert wird. Die Daten werden dann im Rahmen des Einstellungsgespräches und nach dem Abschluss der Ausbildung vom Ministerium für Arbeit und Bau erhoben, wobei die Beantwortung der Fragen freiwillig ist. Die nach Abschluss der Ausbildung erhobenen Daten dienen insbesondere der von der Europäischen Union geforderten Erfolgskontrolle über die geförderte Maßnahme.

Ein Jahr später wurde ich von einer an dem „Ausbildungsplatzprogramm Ost 2001“ beteiligten Stelle gefragt, ob die Voraussetzungen für eine Datenverarbeitung auf freiwilliger Grundlage erfüllt sind. Dies konnte ich bestätigen, da die betroffenen Personen vor der Unterzeichnung des Ausbildungsvertrages nunmehr umfassend informiert werden. Anhand dieser Informationen können sie frei entscheiden, ob sie unter diesen Voraussetzungen die Ausbildung aufnehmen. Darüber hinaus haben sie das Recht, der einmal gegebenen Einwilligung zur Verarbeitung ihrer Daten zu widersprechen.

Diese Stelle sandte mir auch den inzwischen überarbeiteten Erhebungsbogen zu. Dort wird unter anderem nach den konkreten Gründen bei einem Abbruch der Ausbildung gefragt. So sollten die Auszubildenden angeben, ob sie gegebenenfalls wegen einer rechtskräftigen Verurteilung die Ausbildung vorzeitig beendet hätten. Dieses Datum ist meines Erachtens für die Erfolgskontrolle der Förderung nicht erforderlich. Das habe ich dem Ministerium für Arbeit und Bau mitgeteilt und empfohlen, dieses Datum nicht mehr zu erheben. Das Ministerium ist meiner Empfehlung gefolgt.

3.15.2 Videoüberwachung von Hauseingängen

Im Februar 2000 erhielt ich die Information, dass eine kommunale Wohnungsgesellschaft in Hauseingängen einiger Wohnblocks Videokameras installiert hat. Die Aufnahmen werden in einen hauseigenen TV-Kabelkanal eingespeist. Über diesen Kanal können die Mieter jederzeit den Hauseingangsbereich auf ihrem TV-Gerät beobachten. So ist es außerdem möglich, die Bilder beispielsweise über einen Videorecorder elektronisch aufzuzeichnen. Zwar waren die Mieter mit der Überwachung des Eingangsbereiches einverstanden; da aber auf die Videoüberwachung vor diesem Bereich nicht besonders hingewiesen wurde, hatten Dritte, beispielsweise Besucher, keine Kenntnis von der Beobachtung.

Die Beobachtung durch Videokameras sowie die mögliche Aufzeichnung der Bilder durch Mieter stellen einen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen dar. Ob und unter welchen Voraussetzungen der Einsatz von Videotechnik daher ein verhältnismäßiges Mittel ist, den Hauseingangsbereich vor Beschädigungen zu schützen beziehungsweise die Sicherheit der Mieter zu erhöhen, muss in jedem Fall sorgfältig abgewogen werden. Eine Besonderheit des Sachverhaltes besteht zudem darin, dass es darüber hinaus möglich ist, die aufgezeichneten Bilder unkontrolliert zu verbreiten. Mieter könnten die aufgenommenen Bilder an andere Personen weitergeben.

Der Sachverhalt war nach § 22 Kunsturhebergesetz zu bewerten. Danach dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Hier war der Tatbestand des Verbreitens bereits dadurch gegeben, dass die betriebsbereite Kamera jederzeit Bildnisse von Personen, die sich im Hauseingangsbereich befinden, in alle Wohnungen übermittelte. Unter Öffentlichkeit sind hier die Mieter zu verstehen.

Da das Kunsturhebergesetz das Verbreiten eines Bildnisses oder das öffentliche Zur-Schau-Stellen ohne erforderliche Einwilligung gemäß § 33 mit Strafe bewährt, ist diese Einwilligung nicht im datenschutzrechtlichen, sondern im strafrechtlichen Sinne auszulegen. Sie muss deshalb nicht schriftlich erteilt werden, sondern liegt auch dann vor, wenn eine abgebildete Person in Kenntnis der Aufnahme und der Verbreitungsmöglichkeit den Überwachungsbereich betritt und dadurch zum Ausdruck bringt, dass sie mit der Aufnahme und der Nutzung ihres Bildnisses einverstanden ist.

Die Videoüberwachung und die Einspeisung der Aufnahmen in den lokalen TV-Kanal verstoßen somit mangels Einwilligung gegen § 22 Kunsturhebergesetz. Ich habe empfohlen, die Personen, die den Hauseingangsbereich betreten, auf die Videoüberwachung hinzuweisen, damit sie entscheiden können, ob sie sich in den Überwachungsbereich begeben oder nicht. Im Hauseingangsbereich wurde daraufhin ein entsprechender Hinweis angebracht, der Betroffene schon vor dem Erfassungsbereich der Kamera aufklärt.

3.15.3 Umgang mit Kundendaten bei einer Sparkasse

Ein Petent, der Berater einer Campingplatzbetreiberin ist, schilderte mir folgenden Sachverhalt und hat mich gebeten, diesen datenschutzrechtlich zu prüfen:

Im Auftrag der Betreiberin des Campingplatzes hat er bei einer Sparkasse einen Kredit beantragt. Dazu hatte er die erforderlichen Unterlagen eingereicht, unter anderem auch eine detaillierte Auflistung aller Dauercamper. Nach Prüfung der Unterlagen wurde ihm mitgeteilt, dass dem Kreditwunsch nicht entsprochen werden kann. Die Sparkasse schickte deshalb auch die Unterlagen zurück. Der Petent konnte diese Entscheidung nicht nachvollziehen und hat den Vorstand um nochmalige Prüfung des Antrages gebeten, ohne jedoch die Unterlagen erneut vorzulegen. Der Vorstand teilte ihm daraufhin mit, dass die Unterlagen nochmals geprüft worden seien und auch danach dem Kreditwunsch nicht entsprochen werden könne. Den Petenten erstaunte diese Antwort, weil er davon ausgegangen war, dass er seine Unterlagen vollständig zurückerhalten hatte. So vermutete er, dass sie ohne seine Kenntnis kopiert worden sind, und befürchtete, dass sie zu anderen Zwecken genutzt werden könnten. Aus diesem Anlass habe ich den Umgang mit personenbezogenen Daten in der Sparkasse kontrolliert.

In der Kreditabteilung habe ich die Unterlagen abgelehnter Kreditanträge eingesehen. Die Antragsunterlagen der Betreiberin des Campingplatzes waren nicht dabei. Auf Nachfrage teilte mir die Sparkasse mit, dass Kopien dieser Unterlagen zum Zeitpunkt der Kontrolle durch die Rechtsabteilung geprüft worden sind. In der Regel würden aber keine Kopien gefertigt, wenn ein Kreditantrag abgelehnt wird. Die Unterlagen werden nur kopiert, wenn vermutet wird, dass bei einem Kunden der Vorgang später noch einmal geprüft werden müsse, zum Beispiel, wenn er erneut einen Kredit beantragen wird.

Aus datenschutzrechtlicher Sicht ist dieser Sachverhalt wie folgt zu bewerten:

Eine spezielle Vorschrift für das Speichern von Kundendaten nach dem Abbruch von Vertragsverhandlungen existiert nicht. Somit ist der Umgang mit personenbezogenen Daten bei der Sparkasse nach den allgemeinen Bestimmungen des Bundesdatenschutzgesetzes (BDSG) zu bewerten. Danach ist das Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke im Rahmen eines Vertragsverhältnisses oder vertragsrechtlicher Verhandlungen mit der betroffenen Person zulässig (§ 28 BDSG). Falls aber beispielsweise die vorvertraglichen Verhandlungen scheitern, dürfen die Daten nur gespeichert bleiben, wenn rechtliche Auseinandersetzungen darüber zu erwarten sind. Genau dies hat die Sparkasse in der mir vorliegenden Petition geltend gemacht und damit die weitere Speicherung begründet. Ein Verstoß gegen datenschutzrechtliche Bestimmungen lag somit nicht vor.

Um dieses Verfahren für die Kunden jedoch transparent zu gestalten, habe ich der Sparkasse empfohlen, bei einer Ablehnung eines Kreditantrages darüber zu informieren, welche Unterlagen gegebenenfalls kopiert wurden und wie lange sie gespeichert werden. Außerdem sollte zuvor geprüft werden, ob eine Aktennotiz nicht den gleichen Zweck erfüllt. Nur wenn dies nicht der Fall ist, können die erforderlichen Unterlagen im Einzelfall kopiert und zu den Akten genommen werden.

Die Sparkasse hat meine Empfehlungen umgesetzt und ihre Mitarbeiter angewiesen, entsprechend zu verfahren.

3.16 Land-, Forst- und Wasserwirtschaft

3.16.1 Bekanntgabe landwirtschaftlicher Betriebe beim Auftreten von BSE

Ein Abgeordneter bat mich zu prüfen, ob personenbezogene Daten der Landwirte, in deren Rinderherden BSE aufgetreten ist, der Öffentlichkeit bekannt gegeben werden dürfen. Die Medien hatten bereits über solche Landwirte berichtet, während Verarbeitungsunternehmen nicht genannt wurden. Unklar war, woher die Medien diese Informationen erhalten hatten.

Um diesen Sachverhalt zu bewerten, musste ich mir zunächst einen Überblick über den Informationsfluss bei einem BSE-Fall verschaffen. Der Landestierarzt von Mecklenburg-Vorpommern erläuterte in einem Gespräch, welche Stellen Daten des Landwirtes und Daten über die Herkunft des Tieres verarbeiten, wenn ein Rind geschlachtet wird.

Zunächst wird eine amtliche Fleischuntersuchung von einem Tierarzt durchgeführt. Die entnommene Gewebeprobe wird zur Untersuchung an ein Labor versandt, wobei das Labor keine Daten des Landwirtes erhält. Das Labor informiert das Landesveterinäramt über das Ergebnis der Untersuchung. Dort werden diese Daten mit denen des Landwirtes/landwirtschaftlichen Betriebes sowie den Daten über die Herkunft des Rindes zusammengeführt. Wenn die entnommene Probe positiv war, also BSE festgestellt worden ist, informiert das Veterinäramt den Schlachthof. Dieser darf dann das Tier nicht verarbeiten, sondern muss es so entsorgen lassen, dass die Bestandteile nicht in den Nahrungskreislauf gelangen.

Wird BSE festgestellt, ergeht eine offizielle Tierseuchemeldung an die Bundesforschungsanstalt für Tierseuchen in Wusterhausen. Sowohl die Besitzer- als auch die Herkunftsdaten werden übermittelt und dort gespeichert. Die Landwirtschaftsministerien der Bundesländer haben jederzeit Zugriff auf die Daten der BSE-Fälle des eigenen Landes. Sofern ein BSE-Fall aus einem anderen Bundesland abgefragt wird, erhält die anfragende Stelle lediglich den Ort, an dem das Rind vor der Schlachtung lebte, nicht jedoch die Daten des Besitzers. Bloße Verdachtsfälle werden an die Bundesforschungsanstalt für Tierseuchen nicht übermittelt. Darüber hinaus werden auf der Homepage des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft <http://www.bml.de/verbraucher/bse/anzahlbse.htm>) folgende Daten veröffentlicht: BSE-Fallnummer, Seuchenfeststellungsdatum, Bundesland, Landkreis, Geburtsdatum des Rindes, Rinderbestand des Betriebes. Die Daten des Landwirtes/landwirtschaftlichen Betriebes sind – entgegen früherer Vorgehensweise – nicht mehr enthalten.

Aus datenschutzrechtlicher Sicht wäre eine Weitergabe der Daten des Landwirtes/landwirtschaftlichen Betriebes vom Landesveterinäramt an die Medien eine Datenübermittlung an den nicht-öffentlichen Bereich. Diese bedarf entweder einer Rechtsgrundlage oder der Einwilligung der betroffenen Person. Eine entsprechende Rechtsgrundlage für diesen Fall existiert nicht. Zur Befriedigung des öffentlichen Interesses ist es grundsätzlich ausreichend, wenn die zuständige öffentliche Stelle nur erklärt, dass in einer bestimmten Region BSE festgestellt wurde. Dies genügt deshalb, weil bei einem BSE-Fall immer entsprechende Maßnahmen zum Schutz der Bevölkerung eingeleitet werden und daher von dem Landwirtschaftsbetrieb keine unmittelbare Gefahr mehr ausgeht. Auch unser Landwirtschaftsministerium ist der Auffassung, dass personenbezogene Daten des Landwirtes von keinen Stellen an die Medien weitergegeben werden dürfen.

Einen Verstoß gegen datenschutzrechtliche Vorschriften konnte ich bei meiner Recherche nicht feststellen. In einem Fall hat der betroffene Landwirt selbst der Presse mitgeteilt, dass in seinem Betrieb BSE aufgetreten ist. In einem anderen Fall sind die Daten des Landwirtes zwar in der Presse veröffentlicht worden, ohne dass dieser damit einverstanden war. Das Landwirtschaftsministerium hatte dazu aber mitgeteilt, dass die Daten nicht durch eine öffentliche Stelle an die Medien weitergegeben worden sind. Vielmehr haben diese selbst intensiv im Umfeld landwirtschaftlicher Betriebe recherchiert und konnten aus den dabei erhaltenen Anhaltspunkten den Betrieb ermitteln.

Den Abgeordneten habe ich über dieses Ergebnis informiert.

3.17 E-Government

3.17.1 Datenschutzfreundlicher Service in der Verwaltung

Unter dem Stichwort Verwaltungsreform wird seit vielen Jahren eine moderne und bürgerfreundliche Verwaltung gefordert. Dem Bürger soll der Kontakt zur Verwaltung erleichtert werden, und Verwaltungsvorgänge sollen transparenter und schneller ablaufen. Neben der Einrichtung multifunktionaler Verwaltungsdienststellen wie Bürgerbüros wird der elektronischen Datenverarbeitung eine maßgebliche Rolle beigemessen. Moderne Informationstechnik soll dazu beitragen, Anfragen von Bürgern schnell und unbürokratisch zu bearbeiten. Behörden sollen verstärkt die Telekommunikation und insbesondere die Möglichkeiten des Internet für Verwaltungsdienstleistungen nutzen.

Bei dieser Entwicklung sind datenschutzrechtliche Aspekte frühzeitig zu berücksichtigen. Die Bündelung von Verwaltungsaufgaben und der großflächige Einsatz moderner Technik dürfen nicht dazu führen, dass die Trennung von Datenbeständen, die unterschiedlichen Aufgaben zuzuordnen sind, aufgegeben wird. Das gilt vor allem für Daten, die besonderen Geheimhaltungsvorschriften unterliegen, wie Sozial- und Steuerdaten. Werden Daten elektronisch gespeichert und per Telekommunikation übertragen, sind besondere Maßnahmen zum angemessenen Schutz der Vertraulichkeit und der Integrität zu treffen.

Vor diesem Hintergrund haben die Datenschutzbeauftragten des Bundes und der Länder in einer EntschlieÙung vom Oktober 2000 ihre Bereitschaft bekundet, die Modernisierung der Verwaltung zu unterstützen und die hierfür erforderlichen Prozesse konstruktiv zu begleiten (siehe Anlage 8). Eine Arbeitsgruppe hat Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung erstellt, die Ende 2000 in der Broschüre „Vom Bürgerbüro zum Internet“ veröffentlicht wurden.

Diese Broschüre gibt beispielsweise konkrete Hinweise zu Datenschutzfragen bei der Einrichtung von Bürgerbüros. So wird unter anderem darauf hingewiesen, dass Serviceleistungen des Bürgerbüros lediglich Angebote für den Bürger sein können und es keinerlei Verpflichtung geben darf, dort persönliche Daten zu offenbaren. Anträge müssen immer auch beim Fachamt selbst gestellt werden dürfen.

Ausführliche Hinweise gibt es auch zur Zusammenarbeit der öffentlichen Verwaltung mit privaten Call-Centern. In zunehmendem Maße nutzen Verwaltungen diese

Möglichkeit, Dienstleistungen für den Bürger rund um die Uhr anzubieten. Verarbeitet ein Call-Center personenbezogene Daten anfragender Bürger, sind Datenschutzbestimmungen zu berücksichtigen.

Darüber hinaus werden datenschutzrechtliche Anforderungen erläutert, die bei der Nutzung des Internet für Präsentationszwecke von Bedeutung sind (siehe Punkt 3.17.4). Weiterhin werden Rahmenbedingungen für die Anwendung der digitalen Signatur beschrieben (siehe Punkt 3.17.3) und Empfehlungen zum Einsatz von Verschlüsselungsverfahren gegeben.

Die Broschüre ist kostenlos in meiner Dienststelle erhältlich oder kann aus den verschiedenen Internetangeboten der Datenschutzbeauftragten von Bund und Ländern abgerufen werden.

3.17.2 Der rechtliche Rahmen für E-Government

Die öffentliche Verwaltung will in zunehmendem Maße moderne Informations- und Telekommunikationstechnik nutzen, um effektiv und bürgerfreundlich zu arbeiten. Für viele Vorhaben in diesem Bereich ist die rechtliche Gleichstellung der elektronischen Signatur mit der handschriftlichen Unterschrift von entscheidender Bedeutung. So wird beispielsweise ein „elektronischer Verwaltungsakt“ den konventionellen erst dann vollständig ersetzen können, wenn er vom Verwaltungsmitarbeiter rechtskräftig elektronisch unterschrieben werden kann.

Deutschland gehörte weltweit zu den ersten Ländern, die hierfür spezielle Vorschriften erlassen haben. 1997 trat das Informations- und Kommunikationsdienste-Gesetz in Kraft. In Artikel 3 dieses Gesetzes wurden mit dem Signaturgesetz erstmals die Rahmenbedingungen für die Verwendung digitaler Signaturen per Gesetz festgelegt (siehe Dritter Tätigkeitsbericht, Punkt 2.2). Die im selben Jahr verabschiedete Signaturverordnung enthielt die Ausführungsbestimmungen zum Gesetz und regelte technische Details.

Um die im Jahr 1999 verabschiedete Europäische Signaturrechtlinie in nationales Recht umzusetzen, war es notwendig, das Signaturgesetz zu novellieren. Gleichzeitig sollten die Erkenntnisse aus der Evaluierung des Gesetzes berücksichtigt werden. Ende Mai 2001 trat das novellierte Signaturgesetz in Kraft. Gemeinsam mit der im Oktober 2001 vom Bundeskabinett verabschiedeten neuen Signaturverordnung ist

ein wesentlicher Teil des Rechtsrahmens für die Anwendung elektronischer Signaturen in der Verwaltung und in der Wirtschaft geschaffen worden.

Die in diesen Vorschriften normierten Verfahren zur elektronischen Signatur sind von grundlegender datenschutzrechtlicher Bedeutung. Werden diese Regelungen ordnungsgemäß angewendet, sind die Authentizität und Integrität personenbezogener Daten bei der elektronischen Übermittlung sichergestellt. Während das Signaturgesetz von 1997 nur eine technisch sehr aufwändige Form der digitalen Signatur vorsah, bietet das neue Gesetz ein dreistufiges System von elektronischen Signaturen. Mit der Differenzierung zwischen elektronischer, fortgeschrittener elektronischer und qualifizierter elektronischer Signatur ist es möglich, jeweils ein der Sensibilität der zu übertragenden Daten angemessenes Verfahren auszuwählen.

Das Signaturgesetz regelt allerdings nicht, wann elektronische Signaturen zu verwenden sind. Um die digitale Signatur im elektronischen Rechtsverkehr einsetzen zu können, bedarf es weiterer gesetzlicher Vorschriften, die bestimmen, in welchen Fällen die handschriftliche Unterschrift durch die elektronische Signatur ersetzt werden kann:

- Das Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13. Juli 2001 (BGBl. S. 1542) ermöglicht durch Änderungen zahlreicher Gesetze, auch solche Verträge und andere Rechtsgeschäfte elektronisch abzuschließen, für die bisher die Schriftform vorgesehen war. Des Weiteren ändert es die Zivilprozessordnung und Gerichtsordnungen, so dass Anträge und Schriftsätze auch in elektronischer Form bei den Gerichten eingereicht werden können sowie die Echtheit bestimmter digital signierter Erklärungen im Beweisverfahren vermutet wird und dieser Anschein nur unter genau festgelegten Voraussetzungen erschüttert werden kann.
- Das geplante Gesetz zur Anpassung des Verwaltungsverfahrensrechts an die moderne elektronische Kommunikation (Elektronik-Anpassungsgesetz) soll der Verwaltung durch entsprechende Novellierung des Verwaltungsverfahrensgesetzes und der Vorschriften zu speziellen Verwaltungsverfahren die Möglichkeit einräumen, sowohl intern als auch mit dem Bürger elektronisch zu kommunizieren. Die bisher vorliegenden Gesetzentwürfe haben aus datenschutzrechtlicher Sicht jedoch noch Defizite:
- Es fehlt an normenklaren Voraussetzungen dafür, wann die Verwaltung elektronische Dokumente an eine Privatperson schicken darf und diese als zugegangen gelten.

- Es sind keine Regelungen zur Verschlüsselung von elektronischen Dokumenten vorgesehen.
- Die Vorschrift, die die Beglaubigung bei „Medienwechsel“ (Umwandlung der Papierform in elektronische Form und umgekehrt) regelt, ist fehlerhaft und vermischt beispielsweise den Begriff des Zertifikats bei der elektronischen Signatur mit den Inhalten der Beglaubigung.

In diesem Zusammenhang ist auch das am 14. Dezember 2001 verabschiedete Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (EGG) zu nennen. Neben dem Ziel, die Erkenntnisse aus der Evaluierung des Informations- und Kommunikationsdienste-Gesetzes (siehe Dritter Tätigkeitsbericht, Punkt 2.2) durch Novellierung des Teledienstedatenschutzgesetzes zu berücksichtigen (siehe auch 3.9.3), dient das EGG der Umsetzung der EG-Richtlinie über den elektronischen Geschäftsverkehr. Es enthält zwar keine Regelungen zur elektronischen Signatur, aber Änderungen des Teledienstegesetzes, die zu einer Angleichung des Rechts der EG-Mitgliedsstaaten für den elektronischen Geschäftsverkehr führen sowie die Transparenzpflichtungen der Anbieter von Telediensten, deren Verantwortlichkeit für Informationsvermittlung und deren Haftung für im Auftrag von Nutzern gespeicherte Daten detaillierter regeln und verschärfen.

3.17.3 Elektronische Signatur – bald auch in der Verwaltung Mecklenburg-Vorpommerns?

Im Sommer 1999 hatte die Bundesregierung nach langer Diskussion mit Wissenschaftlern und Datenschützern die „Eckpunkte der deutschen Kryptopolitik“ beschlossen. Damit will sie die Verbreitung kryptographischer Verfahren in Deutschland aktiv unterstützen (siehe Vierter Tätigkeitsbericht, Punkt 3.16.2). Es ist erklärtes Ziel der Bundesregierung, die qualifizierte elektronische Signatur (siehe Punkt 3.17.2) flächendeckend zunächst für Anwendungen mit Schriftformerfordernis einzusetzen und somit die Grundlage für die E-Government-Initiative BundOnline 2005 zu schaffen, mit der alle onlinefähigen Dienstleistungen der Bundesverwaltung bis 2005 im Internet angeboten werden sollen. Der Entwurf eines Beschlusses, der die entsprechenden Rahmenbedingungen festlegt und die Strategie der Bundesregierung erläutert, befand sich bei Redaktionsschluss noch in der Ressortabstimmung.

Auch in der Verwaltung unseres Landes ist die Bedeutung von Verschlüsselungs- und Signaturverfahren nunmehr erkannt worden. In seinem Beschluss vom Novem-

ber 2001 weist der Interministerielle Ausschuss für Informations- und Kommunikationstechnik (IMA-IT) „auf die Bedeutung des Projektes Elektronische Signatur/Verschlüsselung hin und bittet die Koordinierungs- und Beratungsstelle der Landesregierung (LKSt), das Projekt federführend fortzusetzen“.

Maßgeblichen Anteil an dieser Entwicklung hat das Justizministerium. Von dort aus wurden meine Forderungen zum Einsatz kryptographischer Verfahren unterstützt (siehe unter anderem Zweiter Tätigkeitsbericht, Punkt 2.16.4 und Vierter Tätigkeitsbericht, Punkt 3.16.2). Das Engagement des Justizministeriums führte unter anderem dazu, dass in den Themenkatalog des Einer-für-Alle-Prinzips (ein Ressort bearbeitet federführend ein ressortübergreifendes Projekt) das oben genannte Projekt „Digitale Signatur und Verschlüsselung“ aufgenommen wurde. Das Ministerium erklärte sich bereit, die Federführung für dieses Projekt zu übernehmen und ein Konzept für die Einführung von Verschlüsselungs- und Signaturverfahren in der Landesverwaltung zu erarbeiten. Die DVZ M-V GmbH wurde beauftragt, ein Positionspapier zu formulieren, das Entscheidungsgrundlage für weitere Aktivitäten der Landesverwaltung auf dem Weg zu einer sicheren Infrastruktur sein soll.

Im April 2001 legte das Justizministerium die Arbeitsergebnisse vor. Neben einem Bericht über Tests verschiedener am Markt verfügbarer Softwarepakete wurde ein Handbuch erarbeitet, das umfangreiche Informationen zum Thema Kryptographie bereitstellt und künftigen Benutzern kryptographischer Verfahren als Nachschlagewerk dienen soll. Das Positionspapier als dritter Teil der Arbeitsergebnisse soll Entscheidungsgrundlage für das weitere Vorgehen sein. In diesem Dokument werden verschiedene Einführungsstrategien vorgeschlagen, relevante Einzelaspekte diskutiert und eine konkrete Vorgehensweise empfohlen. Nach der Bestätigung des Papiers durch den IMA-IT soll demzufolge der Bedarf an kryptographischen Verfahren in der Landesverwaltung ermittelt werden. Die schon mehrfach diskutierte Frage nach dem Aufbau eines landeseigenen oder der Nutzung eines vorhandenen Trustcenters (siehe auch Vierter Tätigkeitsbericht, Punkt 3.16.3) sollte unverzüglich entschieden werden. Danach wären geeignete Hard- und Softwarekomponenten auszuwählen und die Nutzungsmöglichkeiten in konkreten Einsatzumgebungen zu testen.

Parallel zur Planung der technischen Details sind aber auch organisatorische Fragen von entscheidender Bedeutung für den erfolgreichen Einsatz von Signatur- und Verschlüsselungsverfahren. Hier ist der Interministerielle Ausschuss für Organisationsfragen (AfO) gefordert. Beispielsweise muss festgelegt werden, ob künftig jeder Mit-

arbeiter der Landesverwaltung digital signieren soll und ob grundsätzlich alle oder nur ausgewählte Nachrichten zu verschlüsseln sind. Auch ist zu ermitteln, wo die fortgeschrittene digitale Signatur ausreichend ist und welche Bereiche die qualifizierte digitale Signatur erfordern. Insbesondere sind aber alle organisatorischen Fragen zu beantworten, die für die Entscheidung über ein landeseigenes Trustcenter von Bedeutung sind.

Der oben genannte Beschluss des IMA-IT weist zwar in die richtige Richtung, fordert Signatur- und Verschlüsselungsverfahren zunächst jedoch nur bei konkretem und dringendem Bedarf. Da alle Ressorts nachdrücklich diesen Bedarf deutlich gemacht haben, bleibt zu hoffen, dass Kryptographie künftig ein selbstverständliches Standardmerkmal bei der Speicherung und Übermittlung personenbezogener Daten und nach der Klärung einiger organisatorischer Fragen durch den AfO auch ohne Einschränkungen in der Landesverwaltung eingesetzt wird.

3.17.4 Wie sollten sich Behörden im Internet präsentieren?

Der erste Schritt öffentlicher Stellen in Richtung E-Government ist oftmals das Bereitstellen eigener Informationsangebote im Internet. Auf so genannten Homepages finden interessierte Bürger dann beispielsweise Hinweise zu Aufgaben und Öffnungszeiten oder zu Ansprechpartnern für bestimmte Aufgabenbereiche. Auch Informationsmaterialien oder Formulare werden in zunehmendem Maße zum Abruf bereitgehalten. Jedoch berücksichtigen die Behörden bei ihren Veröffentlichungen nicht immer die entsprechenden Rechtsvorschriften.

Datenschutzrechtlich unbedenklich sind Sachdarstellungen ohne Personenbezug. Dazu zählen allgemeine Angaben zur Behörde, Rechtsnormen oder Organigramme ohne Personennamen.

Werden jedoch personenbezogene Daten veröffentlicht, sind datenschutzrechtliche Vorschriften zu beachten. Nach § 31 Landesdatenschutzgesetz von Mecklenburg-Vorpommern (DSG MV) beispielweise dürfen Daten eines Mitarbeiters nur dann öffentlich bekannt gegeben werden, wenn es zur Erfüllung der dienstlichen Aufgabe des Betroffenen erforderlich ist. Daher kommen für eine solche Veröffentlichung meist nur Daten von Mitarbeitern der Leitungsebene oder solchen mit regelmäßigen Außenkontakten in Frage. Daten weiterer Mitarbeiter dürfen nur dann eingestellt werden, wenn diese eingewilligt haben und die Veröffentlichung der Aufgabenerfüllung dient.

Damit Bürger mit den gewünschten Verwaltungsmitarbeitern direkt Kontakt aufnehmen können, reicht es in der Regel aus, im Internetangebot Namen, Funktionen und Tätigkeitsbereiche sowie dienstliche Adressen und Telefonnummern anzugeben. Nicht erforderlich, und ohne Einwilligung des Betroffenen somit nicht zulässig, wäre beispielsweise die Veröffentlichung von Bildern oder Privatanschriften. Dies gilt ebenso für komplette Telefonverzeichnisse oder Geschäftsverteilungspläne mit den Namen aller bei der Behörde Beschäftigten.

Beim Umgang mit den personenbezogenen Daten der Nutzer des Internetangebotes sind bereichsspezifische Vorschriften zu berücksichtigen, die Vorrang vor den allgemeinen Datenschutzgesetzen haben. Dazu zählen vor allem das Teledienstegesetz (TDG) und das Teledienstedatenschutzgesetz (TDDSG), da die Internetangebote öffentlicher Stellen in der Regel als Teledienste anzusehen sind. Aus dem im TDDSG normierten Prinzip der Datensparsamkeit resultiert beispielsweise, dass bei kostenlosen Zugriffen auf das Internetangebot – was bei öffentlichen Stellen der Standardfall ist – keine personenbezogenen Daten der Nutzer wie etwa die E-Mail-Adresse oder die IP-Nummer protokolliert werden dürfen. Nutzungsstatistiken dürfen aus demselben Grund nur einen sehr geringen Detaillierungsgrad aufweisen. Sie dürfen nur anonym oder durch Zusammenfassen von Daten gewonnen werden. Da die öffentliche Stelle Diensteanbieter im Sinne des TDG ist, ist sie zur so genannten Anbieterkennzeichnung verpflichtet. Der Nutzer des Internetangebotes muss also erkennen können, wer der Anbieter der Informationen ist.

Darüber hinaus sollte der Abrufende noch über weitere Details informiert werden. Unter dem Begriff Online-Datenschutz-Prinzipien muss die anbietende Stelle umfassend erklären, wie sie mit den personenbezogenen Daten der Nutzer umgeht, wenn derartige Daten beim Aufrufen der Internetseiten gesammelt werden. Dies gilt insbesondere, wenn Nutzerdaten protokolliert oder in kleinen Dateien auf dem Computer des Nutzers (so genannte Cookies) zur späteren Übermittlung an den Anbieter gespeichert werden. Selbst wenn keine personenbezogenen Daten anfallen, ist es sinnvoll, gut sichtbar auf der Homepage der Behörde die Online-Datenschutz-Prinzipien zu veröffentlichen. Der Nutzer wird auf diese Weise auf das datenschutzfreundliche Angebot hingewiesen, und mögliche Bedenken und Befürchtungen zum Umgang mit seinen Daten werden zerstreut.

Für eine sichere und datenschutzgerechte Veröffentlichung von Informationen im Internet sind neben den oben genannten, vorwiegend organisatorischen, auch technische Maßnahmen zu treffen. So sollte der Web-Server, auf dem die Daten bereitgestellt werden, durch eine Firewall vom Hausnetz der Behörde abgeschottet sein. Es

dürfen nur die Daten abgelegt werden, die tatsächlich für die Veröffentlichung vorgesehen sind. Entwicklungs- und Produktionsumgebung des Web-Angebotes müssen deshalb getrennt werden. Angebote, die nur einem begrenzten Nutzerkreis zugänglich sein sollen, sind durch geeignete technische Maßnahmen vor unbefugtem Zugriff zu schützen. Um Angriffe auf den Web-Server zu erschweren, sollten nur die unbedingt erforderlichen Dienste und Protokolle aktiviert sein. Aus demselben Grund sind Schreibrechte auf das unbedingt notwendige Maß zu reduzieren. Auf die Verwendung aktiver Inhalte wie Java oder ActiveX sollte verzichtet werden, weil dadurch für die Nutzer des Angebotes unnötige Risiken entstehen. Verweise (so genannte Links) auf die Seiten anderer Personen oder Institutionen sollten nur mit Zustimmung des Eigentümers gesetzt werden.

Im Rahmen dieses Tätigkeitsberichtes kann ich nur einen kleinen Ausschnitt des gesamten Themenkatalogs „Veröffentlichungen im Internet“ ansprechen. Detaillierte und ausführliche Informationen zum Thema sind in der „Orientierungshilfe zu Datenschutzfragen der Präsentation von öffentlichen Stellen im Internet“ zu finden, die kostenlos bei mir angefordert oder aus meinem Internetangebot heruntergeladen werden kann. Auch die Broschüre „Vom Bürgerbüro zum Internet“ (siehe Punkt 3.17.1) enthält weitere Hinweise zu diesem Thema.

3.17.5 Datenschutzaspekte von elektronischen Verzeichnisdiensten

Die verstärkte Nutzung neuer Kommunikationsformen wie E-Mail impliziert eine neue Art der Verbreitung der Kommunikationsadressen. Hierzu werden zunehmend elektronische Verzeichnisdienste eingesetzt. Diese sind mit einem in Papierform vorliegenden Adress- und Telefonverzeichnis kaum noch vergleichbar. Einerseits kann auf die Informationen in diesen Verzeichnissen von verschiedenen Stellen aus sehr viel einfacher elektronisch zugegriffen werden. Andererseits werden in der Regel weit mehr personenbezogene und damit datenschutzrelevante Informationen als nur die Adresse eines Kommunikationspartners gespeichert.

Der datenschutzgerechte Betrieb von Verzeichnisdiensten verlangt deshalb zum einen die Berücksichtigung technischer Aspekte, wie die sichere Übertragung personenbezogener Daten. Zum anderen spielen rechtliche Aspekte, wie Inhalt, Form und Zugriff auf die einzelnen Einträge, eine wichtige Rolle. In jedem Fall ist sicherzustellen, dass schutzwürdige Belange der verzeichneten Personen nicht beeinträchtigt werden.

Um öffentlichen Stellen den datenschutzgerechten Umgang mit Verzeichnisdiensten zu erleichtern, hat der Arbeitskreis "Technische und organisatorische Datenschutzfragen" (siehe Punkt 5) die Orientierungshilfe „Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten“ erarbeitet. Sie gibt Empfehlungen zu Verzeichnisdiensten in einer definierten Netzwerkumgebung (Intranet) innerhalb der öffentlichen Verwaltung. Ausführlich wird dort erläutert, welche Gefährdungen für das Recht auf informationelle Selbstbestimmung aus der Aufnahme personenbezogener Daten in einen Verzeichnisdienst für den Betroffenen erwachsen können. So ist nicht auszuschließen, dass diese Daten beispielsweise mit anderen Informationen des Betroffenen zusammengeführt, nicht regelmäßig aktualisiert beziehungsweise berichtet oder einem zu großen Nutzerkreis zur Verfügung gestellt werden. Die Orientierungshilfe enthält darüber hinaus Hinweise zur rechtlichen Einordnung von Verzeichnisdiensten und zur Zulässigkeit der Verarbeitung von Beschäftigtendaten.

Im Ergebnis dieser Betrachtungen wird unter anderem empfohlen, jeden Verzeichniseintrag auf das dienstlich notwendige Minimum zu reduzieren, möglichst enge Zugriffsregelungen zu treffen, die regelmäßige Aktualisierung zu gewährleisten, die Pflege des Verzeichnisdienstes revisionssicher zu protokollieren und den Betroffenen über die Aufnahme seiner Daten in den Verzeichnisdienst zu informieren.

Die Orientierungshilfe ist in der Broschüre „Datenschutz bei der Nutzung von Internet und Intranet“ des Arbeitskreises "Technische und organisatorische Datenschutzfragen" veröffentlicht und in meiner Dienststelle kostenlos erhältlich. Wie alle Publikationen meiner Behörde (siehe Punkt 10) kann der Text auch aus meinem Internetangebot (siehe Punkt 6) heruntergeladen werden.

3.17.6 Internet- und E-Mail-Nutzung am Arbeitsplatz

Immer mehr Mitarbeiter in der öffentlichen Verwaltung haben die Möglichkeit, mit ihrem Arbeitsplatz-PC im Internet zu surfen sowie E-Mails zu verschicken und zu empfangen. Teilweise dürfen sie Internet und E-Mail nicht nur dienstlich, sondern auch privat nutzen. Die Landesregierung teilte mit, dass

- die Internet- und E-Mail-Nutzung durch Dienstvereinbarungen, Dienstanweisungen oder Hausverfügungen geregelt wird, an deren Erstellung der Personalrat mitwirkt,

- bei der Protokollierung in der Regel nicht zwischen privater und dienstlicher Nutzung differenziert wird,
- der Umgang mit den Protokolldaten nur in wenigen Fällen ausreichend geregelt ist und
- die Arbeitsplatz-PC oft nicht mit Verschlüsselungs- und Antivirensoftware ausgestattet sind.

Im Ergebnis habe ich hierzu „Hinweise zur Internet- und E-Mail-Nutzung am Arbeitsplatz“ erarbeitet. Sie basieren auf entsprechenden Empfehlungen des Arbeitskreises Medien der Datenschutzbeauftragten des Bundes und der Länder und ergänzen die „Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“. Die Orientierungshilfe ist unter <http://www.lfd.m-v.de/download/internet.pdf> abrufbar. Vor allem ihr Kapitel 4 „Zulässigkeit von Protokollierung und Inhaltskontrolle mittels einer Firewall“ ist hier relevant.

Die Hinweise

- behandeln grundsätzliche rechtliche Aspekte,
- stellen die Notwendigkeit einer detaillierten und den Mitarbeitern transparenten Regelung des Umgangs mit den Protokolldaten sowie des Vorgehens bei Missbrauch dar,
- beinhalten Empfehlungen zur technischen Ausstattung der Arbeitsplatz-PC und
- beschreiben unterschiedliche Möglichkeiten zulässiger Protokollierungsvarianten und stellen technische Lösungen dazu vor.

Ich habe empfohlen, die in den einzelnen Ressorts bestehenden älteren Regelungen entsprechend zu überarbeiten.

3.18 Technik und Organisation

3.18.1 Das Corporate Network der Landesregierung

Die Landesverwaltung betreibt bislang verschiedene Weitverkehrsnetze (WAN), wie das Landesverwaltungsnetzwerk (LAVINE) und das Ressortverbundnetzwerk der Ministerien oder Sondernetze der Polizei und der Steuerverwaltung. Daneben nutzt die Verwaltung auch öffentliche Fernsprechnetze. Sie hat sich zum Ziel gesetzt, alle diese Netze zu einem einzigen zusammenzufassen – dem Corporate Network (siehe Vierter Tätigkeitsbericht, Punkt 3.16.1). Davon verspricht man sich nicht nur Kostenvorteile, sondern unter anderem auch eine erhöhte Verfügbarkeit der Netzdienste, indem beispielsweise einige bisher sternförmige Netze dann eine maschenartige Struktur erhalten.

Für die Planung und Konzeption des Corporate Network ist – wie für alle ressortübergreifenden Projekte – die Koordinierungs- und Beratungsstelle der Landesregierung für Informations- und Telekommunikationstechnik in der Landesverwaltung (LKSt) im Innenministerium zuständig. Sie hat gemeinsam mit dem künftigen Betreiber, der DVZ M-V GmbH, ein Feinkonzept und ein IT-Sicherheitsrahmenkonzept erarbeitet; ich war in die Beratungen einbezogen worden. Diese Konzepte sind mittlerweile gereift und enthalten unter anderem folgende Aussagen:

- Die sicherheitstechnischen Merkmale sind anhand des IT-Grundschutzhandbuches des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ausgewählt worden und decken somit die Mindestanforderungen ab. Anwender können jedoch auch höhere Sicherheitsanforderungen an die DVZ M-V GmbH richten. Umgekehrt kann auch der Betreiber die Einhaltung von Mindestsicherheitsstandards bei den Anwendern fordern, zum Beispiel den Verzicht auf dezentrale Internetzugänge.
- Die anwendungsspezifischen Netze werden zu Virtuellen Privaten Netzen (VPN) umgestaltet. Übergänge zu externen Netzen wie dem Internet und zwischen den anwendungsspezifischen VPN erhalten zentrale und bei Bedarf auch dezentrale Zugriffsschutzsysteme. Deren Kern wird die bisherige zentrale Firewall für LAVINE bilden.
- Einige Teilnetze, die später im Corporate Network aufgehen sollen, werden bereits mit kryptographischen Mitteln auf der Netzebene geschützt. Für andere VPN ist dies prinzipiell vorgesehen.

Damit ist ein solider Grundstein für den technischen Datenschutz im neuen Corporate Network gelegt; die kryptographischen Sicherheitsmaßnahmen bedürfen jedoch nach wie vor einer Untersetzung, entweder auf der Ebene des VPN oder durch eine ununterbrochene Verschlüsselung zwischen den jeweiligen Personalcomputern (Ende-zu-Ende-Verschlüsselung). Hierzu hat das Justizministerium bereits konkrete Vorarbeiten geleistet (siehe Punkt 3.17.3).

Ein wichtiger Baustein in LAVINE und künftig im Corporate Network ist die zentrale Firewall, die den Übergang zum Internet und zwischen den Ressorts sichert. Diese ist ursprünglich im Auftrage des Justizministeriums aufgestellt worden (siehe Vierter Tätigkeitsbericht, Punkt 3.16.1). Nachdem weitere Ressorts begannen, diese zentrale Sicherheitseinrichtung zu nutzen, wurde das BSI mit deren Prüfung beauftragt.

Das BSI entdeckte einige technische Schwachstellen an der Firewall, die jedoch verhältnismäßig schnell geschlossen werden konnten. Die gewählte Architektur erwies sich als leistungsfähig und sicher. Die Fragen zur Organisation und zur Sicherheit der angeschlossenen Netze und Arbeitsplatzrechner in den Ressorts sind weitaus schwieriger zu lösen.

So hat der Interministerielle Ausschuss Informations- und Kommunikationstechnik (IMA-IT) eine Revisionsgruppe gegründet. Aufgabe dieses Gremiums soll es sein, die notwendige IT-Revision der zentralen Sicherheitseinrichtung zu koordinieren. Auch der Schutz der Arbeitsplatzrechner vor schädlichen aktiven Inhalten aus dem Web ist noch nicht befriedigend gelöst. In vielen Ressorts können nach wie vor alle Bediensteten Java-, JavaScript- oder sogar ActiveX-Elemente mit ihren Browsern laden. Auch der Sicherheitsleitfaden für die Nutzer der zentralen Firewall fehlt bislang.

Diese vor allem organisatorischen Mängel müssen jetzt zügig beseitigt werden. Ich werde die Entwicklung beobachten und die Beteiligten des Projektes weiterhin beraten.

3.18.2 Die TK-Anlage der Landesregierung

Die Telekommunikationsanlage der Landesregierung (TK-Anlage) wird ein zentraler Knotenpunkt im geplanten Corporate Network sein (siehe Vierter Tätigkeitsbericht, Punkt 3.16.1). Deshalb spielt sie bei der Vernetzung der Landesverwaltung eine

entscheidende Rolle. Ein Kontroll- und Informationsbesuch im Innenministerium im April 2000 sollte dazu beitragen, mögliche Sicherheitsmängel bereits vor Einbindung der Anlage in die landesweite Vernetzung festzustellen und gegebenenfalls Vorschläge zur Behebung zu unterbreiten, um Sicherheitsrisiken für das gesamte Netz von vornherein auf ein Minimum zu beschränken.

Zur Vorbereitung der Kontrolle hatte ich deshalb darum gebeten, mir das Sicherheitskonzept für die Anlage zuzusenden. Ein solches Konzept existierte jedoch nicht. Stattdessen erhielt ich einen Katalog von Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aus dem Jahr 1996, der im Ergebnis einer gemeinsam mit dem Innenministerium durchgeführten Schutzbedarfsfeststellung erarbeitet worden war. Darin hatte das BSI die TK-Anlage als hoch schutzbedürftig eingestuft und Sicherheitsmaßnahmen vorgesehen, die das Grundschutzniveau deutlich übersteigen.

Meine Kontrolle zeigte, dass bereits einige Maßnahmen für einen sicheren Betrieb der Anlage erfolgreich umgesetzt waren. Zu nennen sind hier vor allem die Schaffung einer angemessenen sicheren Infrastruktur und der Einsatz von Filtern, die Steuerungsdaten von ISDN-Verbindungen auf ihre Zulässigkeit prüfen (so genannten D-Kanal-Filtern). Diese Filter sind bei ordnungsgemäßer Administration in der Lage, unerwünschte Steuerinformationen herauszufiltern, um den Missbrauch der zur Steuerung der Anlage vorgesehenen D-Kanäle zu verhindern.

Erhebliche Mängel zeigten sich jedoch insbesondere im organisatorischen Bereich. So fehlten wichtige vom BSI geforderte organisatorische Hilfsmittel zum sicheren Betreiben der TK-Anlage. Dazu gehörte beispielsweise neben einem aussagekräftigen Sicherheitskonzept auch das zur regelmäßigen Überprüfung der TK-Anlage erforderliche Revisionskonzept. Die ebenfalls für Zwecke der Revision notwendige Dokumentation der gesamten Anlage war nicht auf dem aktuellen Stand. Die Stelle für einen Revisionsbeauftragten war zwar eingerichtet worden, zum Zeitpunkt der Kontrolle aber noch nicht besetzt. Handlungsanweisungen zum Umgang mit der TK-Anlage im Havariefall lagen nur in Ansätzen vor.

Aber auch im technischen Bereich zeigten sich Schwachstellen. Der Administrationsarbeitsplatz als sicherheitstechnisch bedeutsame Schnittstelle zur TK-Anlage muss vor Missbrauch besonders geschützt werden. Dieser Computer war jedoch nicht im sehr gut geschützten Bereich der Anlage untergebracht und darüber hinaus lediglich über das Hausnetz des Innenministeriums an die TK-Anlage angebunden. Dies genügte nicht den Anforderungen des BSI. Auch die Verbindung zwischen der TK-Anla-

ge des Innenministeriums als zentralem Knotenpunkt und den Anlagen in den anderen Ministerien war nicht befriedigend. Durch technische Vorkehrungen wird zwar die unberechtigte Einwahl in den Anlagenverbund verhindert. Die Vertraulichkeit der Kommunikation zwischen den einzelnen Teilanlagen ist aber nur bedingt gewährleistet. Die Daten werden während der Übertragung zwischen den Anlagen auf den hierfür verwendeten öffentlichen Standleitungen der Deutschen Telekom AG nicht verschlüsselt, obwohl das BSI dies ausdrücklich für diese Art von Verbindungen empfohlen hat.

In seiner Stellungnahme zum Kontrollbericht sagte der Innenminister zu, meine Empfehlungen umzusetzen. Er hat allerdings darauf hingewiesen, dass nicht alle Maßnahmen sofort umsetzbar wären, da zunächst die personellen und finanziellen Voraussetzungen geschaffen werden müssten. Deshalb wurde ein Zeitplan zur Umsetzung der erforderlichen Maßnahmen erarbeitet, der in enger Abstimmung mit dem BSI sukzessive abgearbeitet wird.

Im März 2001 teilte der Innenminister folgenden Umsetzungsstand der im Zeitplan festgeschriebenen Maßnahmen mit:

- Im Juli 2000 wurde die Stelle des Revisors besetzt.
- Der Administrationsarbeitsplatz wurde im Januar 2001 in den Bereich der TK-Anlage verlegt.
- Anfang Mai 2001 lag die erste Version des Sicherheitskonzeptes vor.
- Erweiterte Anweisungen zur Störungsbeseitigung und ein überarbeiteter Notfallplan wurden in das Sicherheitskonzept integriert.
- Die Arbeiten zur Erstellung des Revisionskonzeptes sollten im dritten Quartal 2001 abgeschlossen werden.

Dieser Arbeitsstand zeigt, dass dem datenschutzgerechten und sicheren Betrieb der TK-Anlage ein hoher Stellenwert beigemessen wird. Die vollständige Abarbeitung des Maßnahmeplans wird jedoch noch einige Zeit in Anspruch nehmen. Insbesondere vor dem Hintergrund der geplanten Einbindung der TK-Anlage in das Corporate Network der Landesverwaltung werde ich auch weiterhin zum datenschutzgerechten Betrieb der Anlage beraten und die vollständige Umsetzung der Maßnahmeempfehlungen begleiten.

3.18.3 Telearbeit – woran man denken sollte

Im Zeitalter der modernen Informations- und Kommunikationstechnik gewinnt die Telearbeit auch in Behörden an Bedeutung. Sie kann dazu beitragen, die Arbeitsorganisation flexibler zu gestalten, Kosten einzusparen sowie Beschäftigten wohnortnahe Arbeitsplätze und flexiblere Arbeitszeiten anzubieten. Unsere Landesregierung hat in der Verordnung über die Arbeitszeit von Beamten in Mecklenburg-Vorpommern (Arbeitszeitverordnung – AZVO) die Möglichkeit der Telearbeit eingeräumt.

An den Umgang mit personenbezogenen Daten im Rahmen der Telearbeit sind aus datenschutzrechtlicher Sicht hohe Anforderungen zu stellen, weil das Gefährdungspotential bei der Datenverarbeitung außerhalb der Dienststelle größer ist. Insbesondere müssen die Rechtmäßigkeit, Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung nicht nur ständig gewährleistet, sondern auch regelmäßig überwacht werden können (Organisationskontrolle). Die Daten verarbeitende Stelle stößt bei der Durchsetzung dieser Pflichten auf grundsätzliche Schwierigkeiten, da sie bei einem Telearbeitsplatz nicht mehr wie in der Dienststelle die uneingeschränkte Organisationsgewalt über Hard- und Software, Datenbestände und handelnde Personen hat.

Für Telearbeitsplätze ist kennzeichnend, dass personenbezogene Daten die Daten verarbeitende Stelle verlassen und die Verarbeitung zunächst faktisch nur noch eingeschränkt beaufsichtigt werden kann. Von besonderer Bedeutung ist dabei, dass bei Telearbeitsplätzen in der Regel die infrastrukturellen Sicherungsmaßnahmen fehlen, die bei dienststelleninternen Arbeitsplätzen Standard sind. Am Heimarbeitsplatz sind darüber hinaus weder Datenschutz- noch IT-Fachleute präsent, so dass die regelmäßige Überprüfung der richtigen Funktionsweise der Telearbeitsplätze nur schwer realisierbar ist. Hinzu kommt, dass Kontrollen des Dienstherrn oder der zuständigen Datenschutzkontrollinstanzen (Landesdatenschutzbeauftragter oder behördlicher Datenschutzbeauftragter) im häuslichen Umfeld ohne Einwilligung des Telearbeiters nicht möglich sind und somit die Organisationsgewalt der Daten verarbeitenden Stelle weiter eingeschränkt wird.

All das führt bei Telearbeit zu einem ungleich größeren Risiko der möglichen Beeinträchtigung des Rechtes auf informationelle Selbstbestimmung der von einer derartigen Datenverarbeitung Betroffenen. Datenschutzrechtliche Überlegungen zum Thema Telearbeit müssen deshalb die Minimierung dieses zusätzlichen Risikos zum Ziel haben.

Aus datenschutzrechtlicher Sicht sind bei der Telearbeit vor allem drei Aspekte von Bedeutung:

- Je nach **Art der zu verarbeitenden Daten** sind unterschiedlich starke Einschränkungen zu beachten. Wegen der oben genannten Besonderheiten eines Telearbeitsplatzes dürfen sensible personenbezogene Daten nur unter bestimmten Voraussetzungen außerhalb der Dienststelle verarbeitet werden. Das betrifft insbesondere die Daten, die einem besonderen Amts- oder Berufsgeheimnis unterliegen.
- Telearbeit kann die **Privatsphäre der Bediensteten** nachhaltig beeinflussen. So könnten Telearbeitsplätze beispielsweise als umfassende Informationsquellen über die Arbeitsweise von Bediensteten „missbraucht“ werden, da ein außerordentliches Potential für die Sammlung, Messung und Auswertung von Daten sowohl über die Leistungsfähigkeit als auch über andere persönliche Eigenschaften besteht.
- Telearbeitsplätze werden **außerhalb üblicher Büroumgebungen** eingerichtet. Der Datenaustausch mit der Dienststelle erfolgt in der Regel über öffentliche Leitungen. Es sind deshalb angemessene technische und organisatorische Maßnahmen zum Schutz der Vertraulichkeit und der Integrität sowohl der zu übertragenden als auch der am Telearbeitsplatz und der in der Zentrale zu speichernden personenbezogenen Daten zu treffen.

Um öffentliche Stellen zu Datenschutzfragen bei Telearbeitsplätzen zu informieren, habe ich die Orientierungshilfe „Datenschutz bei Telearbeit“ erstellt. Sie erläutert, unter welchen Voraussetzungen Telearbeitsplätze datenschutzgerecht eingerichtet und betrieben werden können und welche rechtlichen und technischen Anforderungen dabei zu beachten sind. Darüber hinaus gibt sie Hinweise zur Ausgestaltung einer entsprechenden Dienstvereinbarung und zur Formulierung der erforderlichen Einzelverträge zwischen Telearbeiter und Dienststelle.

Die Orientierungshilfe ist in meiner Dienststelle kostenlos erhältlich und kann aus meinem Internetangebot (siehe Punkt 6) heruntergeladen werden.

3.18.4 Ein Personalcomputer in mehreren Netzen?

In immer mehr Behörden erhalten die Bediensteten Zugang zum Internet oder benötigen zur Erfüllung ihrer Aufgaben den Zugriff auf mehrere Dienste und Anwendungen

gen, beispielsweise Internet, elektronische Post, Dokumentenverwaltung und Fachanwendungen. Häufig sind die damit verarbeiteten Daten unterschiedlich schutzbedürftig; bei gemeinsamer Nutzung auf einem Arbeitsplatz können aber von einer Anwendung Gefahren für andere ausgehen.

Gelangt zum Beispiel über den Internetzugang unerwünschte Software, etwa ein Trojanisches Pferd, auf einen Arbeitsplatzrechner, auf dem auch ein Personalverwaltungssystem läuft, dann ist die Vertraulichkeit der Personaldaten gefährdet. Eine vergleichbare Situation ist beim Einsatz des HKR-Verfahrens PROfiskal gegeben (siehe Punkt 3.10.4).

Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten im Verwaltungsnetz oder in einem Teilnetz müssen auch unter diesen Umständen hinreichend gewährleistet sein. Angriffe dürfen weder über offene Verbindungen noch mit Trojanischen Pferden, die über E-Mail oder aktive Inhalte eingeschleust werden, erfolgreich sein.

Dass diese Fragen gelöst werden können, zeigt das Beispiel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD). Hier wird eine Musterlösung vorgestellt, die dort selbst betrieben wird, um Internetdienste auch im eigenen Verwaltungsnetz nutzen zu können. Dabei wird vorrangig Open-Source-Software eingesetzt (siehe Punkt 3.18.6).

Zunächst wurde dort eine klassische Firewall aus Paketfiltern und Application Level Gateway aufgebaut, wie in der Orientierungshilfe Internet beschrieben (siehe Vierter Tätigkeitsbericht, Punkte 3.16.4 und 4). Zentrale Ressourcen wie Web- und Mail-Server sind in der Demilitarisierten Zone (DMZ) dieses Systems platziert. Mögliche Sicherheitsverletzungen werden mit Hilfe eines speziellen Protokollierungscomputers (Log-Server) registriert und ausgewertet. Internetzugriffe vermittelt ein so genannter VNC-Server. VNC (Virtual Network Computing) trennt den Arbeitsplatzrechner von den Anwendungen. Auf dem Server laufen alle Programme, die für die Internetnutzung erforderlich sind, wie E-Mail-Programm, Web-Browser oder auch eine Textverarbeitung; der Arbeitsplatzrechner hingegen führt nur ein einfaches Clientprogramm aus. Client und Server tauschen ausschließlich Daten über Tastenanschläge, Mausbewegungen und Bildschirminhalte aus. Ferner kann man vom VNC-Server aus noch auf einen Computer zugreifen, der beispielsweise E-Mails verschlüsselt speichert (PGP-Server).

Die Lösung zeichnet sich durch folgende Eigenschaften aus:

- Aktive Inhalte aus dem Internet wie Java oder JavaScript brauchen nicht auf dem Arbeitsplatzrechner ausgeführt zu werden. Auch die teilweise komplexen Programme zur Nutzung des Internet laufen nur auf dem Server. Sicherheitsrelevante Fehler in diesen Programmen wirken sich nicht auf den Arbeitsplatzrechner und das Verwaltungsnetz aus.
- Anwendungen aus verschiedenen Netzen, wie dem Verwaltungsnetz und dem Internet oder auch dem Netz einer Fachanwendung, können voneinander isoliert werden.
- Wird der VNC-Server trotz der Firewall manipuliert, so ist die Sicherheit des Verwaltungsnetzes noch nicht verletzt. Auf die im Verwaltungsnetz verarbeiteten Daten kann man vom VNC-Server aus nicht zugreifen.
- Die einfache Client-Software ist wenig anfällig gegenüber Fehlern und Manipulationsversuchen.
- Die Protokolldaten auf dem Log-Server werden nach dem Vier-Augen-Prinzip verwaltet.
- Der Datenaustausch zwischen den Netzen wird über die Zwischenablage ermöglicht. Vom VNC-Server aus kann man Dokumente auf einem Netzwerkdrucker ausgeben.
- Ferner sind die Anforderungen an die Client-Hardware gering, denn die Client-Software braucht nur geringe Ressourcen.
- Es ist möglich, mehrere VNC-Server parallel zu betreiben, um mehr Arbeitsplätze bedienen zu können. Jedoch sollten die Server über ausreichend Hauptspeicherkapazität verfügen, und die Netzlast sollte in geeigneter Weise verteilt werden.

Dieses Verfahren gewährleistet insgesamt ein hohes Schutzniveau. Dabei bleiben die Anforderungen an die Hardware relativ gering, und die Software ist sogar kostenlos, jedoch ist ein gewisser personeller Aufwand für Einrichtung und Betrieb einzuplanen. Es ist aber denkbar, Teile des Firewallsystems durch einen Auftragnehmer betreuen zu lassen.

Auch in Mecklenburg-Vorpommern sind bereits einige öffentliche Stellen an der Nachnutzung interessiert. In meiner Dienststelle ist der Einsatz ebenfalls vorgesehen.

3.18.5 Prüfkriterien für datenschutzfreundliche Produkte

In meinem Vierten Tätigkeitsbericht habe ich unter Punkt 3.16.6 über den internationalen Kriterienkatalog „Common Criteria 2.0“ berichtet, mit dem unter anderem nun auch datenschutzspezifische Anforderungen an Hard- und Softwareprodukte beschrieben werden können. In den Common Criteria ist detailliert festgelegt, wie diese Anforderungen zu formulieren sind. Ein wichtiges Hilfsmittel sind so genannte Schutzprofile (Protection Profiles). Sie ermöglichen beispielsweise künftigen Anwendern von Hard- und Softwareprodukten eine konkrete, formalisierte Beschreibung der eigenen Anforderungen.

Auch die Datenschutzbeauftragten des Bundes und der Länder wollen diese Hilfsmittel nutzen, um allgemeingültige, datenschutztechnische Anforderungen an Hard- und Softwareprodukte zu beschreiben. Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (siehe Punkt 5) hat deshalb eine Arbeitsgruppe mit der Ausarbeitung eines Schutzprofils beauftragt, das ein Datenschutz- und Datensicherheitsmodul beschreibt, mit dem sensible Daten – beispielsweise aus dem medizinischen Bereich – verschlüsselt, digital signiert oder pseudonymisiert werden können.

Die Arbeitsgruppe tagte unter der Federführung meines bayerischen Kollegen mehrmals beim Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn. Das BSI hatte einen Mitarbeiter als ständiges Mitglied in die Arbeitsgruppe entsandt und für effektive organisatorische Rahmenbedingungen gesorgt. Beispielsweise wurden die Mitglieder der Arbeitsgruppe, unter ihnen auch ein Mitarbeiter meiner Dienststelle, in einem zweitägigen Seminar kostenlos in die Common Criteria eingewiesen und in deren Anwendung und Handhabung ausgebildet.

Ursprünglich sollte das Schutzprofil lediglich beschreiben, wie die aus der Gesundheitsreform 2000 resultierenden Anforderungen an den Datenaustausch zwischen Ärzten und Leistungserbringern sichergestellt werden können (siehe dazu Vierter Tätigkeitsbericht, Punkt 3.10.1). Im Laufe der Entwicklung zeigte sich jedoch, dass das beschriebene Modul nicht nur im medizinischen Bereich, sondern beispielsweise auch bei Tele- und Mediendiensten, bei E-Commerce-Anwendungen und in Data-Warehouse-Konzepten (siehe Punkt 4.5) einsetzbar sein wird. Der Entwurf wurde daraufhin verallgemeinert, vervollständigt und weitgehend ausformuliert. Mitte des Jahres 2000 legte die Arbeitsgruppe mit dem Entwurf des Schutzprofils „Datenschutz- und Datensicherheitsmodul“ ein erstes Zwischenergebnis vor. In diesem Entwurf wird in der formalisierten Sprache der Common Criteria beschrieben, wie der Informationsfluss beim elektronischen Datenaustausch zwischen mehreren Kommunika-

tionsteilnehmern mit kryptographischen Methoden so gesichert werden kann, dass Authentizität, Vertraulichkeit und Integrität der übertragenen Daten gewährleistet sind.

Mit der Vorlage des Entwurfes beendete die Arbeitsgruppe zunächst ihre Tätigkeit, da die fachlichen und zeitlichen Möglichkeiten nahezu ausgeschöpft waren. Für die weiterführenden Arbeiten – insbesondere die detaillierte Beschreibung der so genannten Funktionalen Sicherheitsanforderungen – war unter anderem sehr detailliertes Fachwissen im Bereich der Standardisierung erforderlich. Ich habe deshalb das BSI um weitere Unterstützung gebeten. Das BSI erklärte sich bereit, den Entwurf des Schutzprofils zu vervollständigen. Es initiierte hierfür ein eigenes Projekt und beauftragte mit dem Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI) einen kompetenten Partner mit der Fortführung der Arbeiten. Das gesamte Projekt wird weiterhin vom BSI sachkundig begleitet. Mein bayerischer Kollege wird in die Arbeiten einbezogen, so dass die datenschutztechnische Ausrichtung des Schutzprofils auch weiterhin sichergestellt ist.

3.18.6 Open-Source-Software datenschutzfreundliche Technologie?

Die Datenschutzbeauftragten des Bundes und der Länder setzen sich seit geraumer Zeit für die Nutzung datenschutzfreundlicher Technologien ein. Unter anderem fordern sie Softwareanbieter auf, Programme so zu entwickeln, herzustellen und zu publizieren, dass Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit der Sicherheitsvorkehrungen überzeugen können. Unabhängige Fachleute müssen die Funktionsweise lückenlos nachvollziehen und fehlerhaft arbeitende Teilkomponenten finden können.

Derartige Transparenz von Software kann dann gewährleistet werden, wenn Quelltexte von Programmen nicht geheim gehalten, sondern für Prüf- und Revisionszwecke zugänglich gemacht werden. Solche Kontrollmechanismen sind unerlässlich, weil komplexe Software praktisch kaum fehlerfrei ist und – wie die Erfahrung zeigt – die Qualitätskontrollen der Hersteller häufig nicht ausreichen.

Ein vielversprechender Ansatz für Transparenz als eine Form datenschutzfreundlicher Technologien stellt das Entwicklungsmodell “Open Source” dar. Unter Open-Source-Software (OSS) versteht man Software, deren Quelltext (source code) offengelegt und frei verfügbar ist. Jeder könnte somit prinzipiell den Quelltext lesen, mit ihm arbeiten, ihn verbessern und solche Änderungen uneingeschränkt publizieren.

In der Regel werden jedoch sowohl Benutzer als auch die meisten Programmierer fachlich nicht in der Lage sein festzustellen, ob ein bestimmtes Programm sicher ist. Nur ein kleiner Kreis von speziellen Fachleuten wird prüfen können, ob Software tatsächlich die angegebenen Funktionen realisiert und darüber hinaus keine Programmteile enthält, die unerwartete und meist unerwünschte Funktionen ausführen (etwa so genannte Trojanische Pferde) oder die spätere Eindringmöglichkeiten in das System („Hintertüren“) eröffnen. Um die Funktionsweise von Programmen vollständig zu überblicken, sind neben dem Quelltext auch verständliche Kommentare und Programmdokumentationen zu veröffentlichen.

Damit Anwender dem Urteil dieser Fachleute vertrauen können, ist die Software nach vorgegebenen Kriterien zu prüfen. Evaluation und Zertifizierung nach international gültigen Kriterienkatalogen (beispielsweise nach den Common Criteria – siehe Vierter Tätigkeitsbericht, Punkt 3.16.6) sind deshalb notwendige Hilfsmittel, um der Open-Source-Software berechtigtes Vertrauen entgegenbringen zu können. Für den „normalen“ Anwender bringt die Offenlegung von Software und Dokumentationen erst dann zusätzliche Sicherheit, wenn er sich davon überzeugen kann, dass eine Prüfung bereits erfolgt ist. Ihm selbst nützt vor allem eine verständliche Programmbeschreibung, die beispielsweise zeigt, wie Sicherheitsfunktionen aktiviert werden.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (siehe Punkt 5) hat im Auftrag der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ein Arbeitspapier zum Thema „Transparente Software“ erstellt, in dem das Open-Source-Modell aus datenschutztechnischer Sicht bewertet wird und Hinweise zum Einsatz in der öffentlichen Verwaltung gegeben werden.

Auch die Verwaltung unseres Landes strebt an, in zunehmendem Maße Open-Source-Software einzusetzen. Die Koordinierungs- und Beratungsstelle der Landesregierung (LKSt) hat einen Fragenkatalog entworfen, auf dessen Basis Nutzungsmöglichkeiten für Open-Source-Software aufgezeigt, der Aufwand abgeschätzt und Anpassungsstrategien entwickelt werden sollen. Diese Entwicklung ist zu begrüßen.

3.18.7 Drahtlose Vernetzung – noch nicht zu empfehlen

Im Jahr 2001 hat mich die Datenschutzbeauftragte einer öffentlichen Stelle gebeten, sie zum Einsatz von Funknetzen (WLAN) nach dem Standard IEEE 802.11b zu be-

raten. Diese mittlerweile von verschiedenen Herstellern angebotene Technik kann drahtgebundene lokale Netze ersetzen. Die Vernetzung von Notebooks oder Geräten, deren Standort mit konventioneller Verkabelung schwer erreichbar ist, kann mitunter wesentlich erleichtert werden. Darüber hinaus ist die Installation eines drahtlosen Netzes oft preiswerter als eine herkömmliche Verkabelung.

Die Hersteller von Netzkomponenten werben damit, dass solche drahtlosen Netze ebenso sicher sind wie drahtgebundene. Dies soll unter anderem das im Standard enthaltene kryptographische Protokoll mit dem Namen „WEP“ (wired equivalent privacy) gewährleisten. Fachleute haben die Sicherheit von Funknetzen in letzter Zeit genauer untersucht und sind unter anderem zu folgenden Ergebnissen gekommen:

- Mit entscheidend für die Sicherheit von Verschlüsselungsverfahren ist die Länge der verwendeten Schlüssel. Sie ist maßgeblich für die größtmögliche Anzahl verschiedener Schlüssel und damit ein Maß für den Aufwand, der für das Brechen des Algorithmus erforderlich ist. Im WEP-Standard ist zum Verschlüsseln der Daten nur ein 40 Bit langer Schlüssel vorgesehen. Damit ist nicht auszuschließen, dass der jeweils verwendete Schlüssel durch Probieren ermittelt wird. Auch wenn die von vielen Herstellern inzwischen angebotenen 104 Bit langen Schlüssel – die Firmen geben 128 Bit an – genutzt werden, bleibt ein weiterer Angriffspunkt. Diese Schwachstelle ist eine im Standard vorgesehene Hilfsgröße, der so genannte Initialisierungsvektor. Dieser Parameter braucht zwar nicht geheim gehalten zu werden wie ein Schlüssel. Für eine sichere Verschlüsselung müsste er sich jedoch mit jedem ausgesandten Datenpaket ändern und darf sich nicht wiederholen. Der Initialisierungsvektor ist jedoch nur 24 Bit lang. Schon nach wenigen Betriebsstunden des Funknetzes ist somit die Menge der möglichen Werte aufgebraucht, so dass mit Wiederholungen zu rechnen ist. Einige Produkte lassen diese Größe sogar konstant und fördern damit ein noch schnelleres Brechen. Im Internet sind bereits Programme verfügbar, mit denen man diese Schwachstelle ausnutzen kann.
- Jedes Datenpaket enthält einen Wert, mit dem man die Integrität prüfen kann. Dieser wird jedoch nach einem Verfahren berechnet, welches nur zufälligen Störungen wirksam begegnet. Manipuliert jemand nun einzelne Bits des Pakets, kann er genau bestimmen, welche Bits er in dem Prüfwert ändern muss. Auf diese Weise kann er gefälschte Pakete aussenden, deren Ungültigkeit das System nicht erkennt.
- Unbefugte können die so genannten MAC-Adressen (Geräteadressen) auf einen gültigen, im System verwendeten Wert einstellen. Zwar sollen sich umprogrammierte Adressen von WLAN-Karten an einem speziellen Bit erkennen lassen, je-

doch ist dies lediglich eine Funktion des Original-Gerätetreibers. Da auch andere Treiber verfügbar sind, ist diese Schutzvorkehrung wirkungslos und der unbenmerkte Betrieb nicht zugelassener Endgeräte im Funknetz möglich.

Wegen dieser Schwachstellen entspricht das Sicherheitsniveau drahtloser lokaler Netze nach IEEE 802.11b lediglich dem des Internet. Obwohl die vom Standard vorgesehenen Sicherheitsmaßnahmen wie WEP-Verschlüsselung oder Festlegung und Prüfung der MAC-Adressen nur ein sehr geringes Schutzniveau bieten, sollten sie genutzt werden. Vertraulichkeit und Integrität können jedoch nur mit zusätzlichen, über den Standard hinausgehenden Maßnahmen sichergestellt werden. Der Anschluss solcher Funknetze sollte deshalb – genau wie der des Internet – nur über eine Firewall erfolgen. Zusätzlich sind die im Funknetz übertragenen Daten auf höheren Netzwerkschichten zu verschlüsseln, zum Beispiel mit IPSec. Wegen der beschriebenen Schwachstellen dürfen die WLAN-Verteiler (so genannte access points) nicht über die drahtlose Schnittstelle konfiguriert und verwaltet werden.

Die Landeskoordinierungsstelle für Informations- und Kommunikationstechnik (LKSt) ist der vorausgehenden Bewertung gefolgt. Sie empfiehlt im IT-Strukturrahmen des Landes Mecklenburg-Vorpommern, WLANs nur einzusetzen, „sofern Vertraulichkeit und Integrität mit zusätzlichen Maßnahmen sichergestellt werden oder nur geringe Sicherheitsanforderungen bestehen“.

3.18.8 Datenschutzfreundliche Videoüberwachung?

Die Zahl von Videokameras zur Überwachung nimmt ständig zu. Ob auf Flughäfen, Bahnhöfen, in Ladenpassagen, Schalterhallen von Banken oder anderen der Öffentlichkeit zugänglichen Einrichtungen – überall müssen Bürgerinnen und Bürger damit rechnen, dass sie auf Schritt und Tritt offen oder heimlich von einer Videokamera aufgenommen werden (siehe auch Punkt 3.15.2). Auch wenn der Einsatz von Videotechnik im Einzelfall durchaus gerechtfertigt erscheinen kann, darf nicht außer acht gelassen werden, dass jede einzelne Kamera ein weiterer Schritt zu einer flächendeckenden Überwachungsinfrastruktur ist.

Mit der Videoüberwachung sind hohe Risiken für das Recht auf informationelle Selbstbestimmung verbunden. Weil eine Videokamera alle Personen erfasst, die in ihren Bereich kommen, werden von der Videoüberwachung unvermeidbar auch völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen betroffen. Erfassung, Aufzeichnung und Übertragung von Bildern sind für die Einzelnen in aller

Regel nicht durchschaubar. Schon gar nicht können sie die durch die fortschreitende Technik geschaffenen Bearbeitungs- und Verwendungsmöglichkeiten abschätzen und überblicken. Die daraus resultierende Ungewissheit, ob und von wem sie beobachtet werden und zu welchen Zwecken dies geschieht, erzeugt einen latenten Anpassungsdruck. Dies beeinträchtigt nicht nur die grundrechtlich garantierten individuellen Entfaltungsmöglichkeiten, sondern auch das gesellschaftliche Klima in unserem freiheitlichen und demokratischen Gemeinwesen insgesamt. Alle Menschen haben das Grundrecht, sich in der Öffentlichkeit frei zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.

Um die ständig zunehmenden Anfragen zum Thema kompetent beantworten und zu den vielen neuen Projekten angemessen beraten zu können, ist es nötig, die technischen Möglichkeiten dieser modernen Überwachungstechnik zu kennen und ihre Eingriffstiefe in die Privatsphäre beurteilen zu können. Vor diesem Hintergrund habe ich im November 2000 die Fachkonferenz „Grenzen und Risiken der Videoüberwachung“ in Schwerin durchgeführt. Anwender, Politiker, Datenschützer, Techniker, Wissenschaftler und Fachjournalisten berieten über Nutzen und Risiken von Videoüberwachungstechnik. Insbesondere konnten Anwender aus der Praxis der Videoüberwachung berichten, Wissenschaftler und Techniker die Leistungsfähigkeit moderner Videotechnik und Verfahren zur Erkennung von Personen durch körpereigene Merkmale (biometrische Verfahren) demonstrieren. Datenschützer zeigten mögliche Schranken der Verwendung derartiger Systeme auf.

Ein Schwerpunkt der Veranstaltung war die Vorstellung verschiedener Produkte und Verfahren, die zur Videoüberwachung, zur Bilderkennung oder zur Identifikation einzelner Personen mit Hilfe biometrischer Verfahren eingesetzt werden können. Die Leistungsfähigkeit dieser modernen Technik konnte während der Fachkonferenz eindrucksvoll demonstriert werden. Die Darstellung verschiedener Pilotversuche zur Videoüberwachung und zur Anwendung biometrischer Verfahren lässt nur erahnen, mit welchen Überwachungsmöglichkeiten künftig zu rechnen ist.

Erfreulicherweise hatten sich einige Hersteller aber auch Gedanken darüber gemacht, wie Videoüberwachung ausgestaltet werden kann, um den Eingriff in die Privatsphäre insbesondere für unbescholtene Bürger so weit wie möglich zu reduzieren. So wurde gezeigt, dass es durchaus technische Maßnahmen gibt, die das Recht auf informationelle Selbstbestimmung in gewissen Grenzen schützen können. Beispielsweise wurden Kamerasysteme vorgestellt, bei denen bestimmte Bildbereiche programmtechnisch ständig ausgeblendet werden. Weiterhin wurde erläutert, wie besonders datenschutzrelevante Leistungsmerkmale von Videokameras wie die Zoomfunktion oder der Aufzeichnungsmodus durch Codesysteme gesperrt und somit nur

speziell autorisierten Nutzern zugänglich gemacht werden können. Es wurden Zutrittskontrollsysteme für Videoleitstellen und Zugriffsschutzeinrichtungen für Bildspeicher gezeigt. Auch wurde die Absicherung der Übertragung von Videodaten von den Kameras zu den Leitstellen, beispielsweise durch Verschlüsselung, vorgestellt. Schließlich wurde über automatische Protokollierungskomponenten und die zeitgesteuerte Löschung nicht mehr benötigter Bilder berichtet.

Im Ergebnis der Veranstaltung wurde zwar deutlich, dass es eine „datenschutzfreundliche Videoüberwachung“ nicht geben kann. Durch die oben beschriebenen Schutzvorkehrungen ist es jedoch möglich, die Beeinträchtigung der Privatsphäre zu reduzieren. Es bleibt zu hoffen, dass bei der weiteren Entwicklung von Videotechnik nicht nur die Überwachungsmöglichkeiten perfektioniert werden, sondern dem Schutz der Privatsphäre unbescholtener Bürger beim Einsatz dieser Technik ebensoviel Aufmerksamkeit geschenkt wird.

4

FORTSETZUNG VON THEMEN FRÜHERER TÄTIGKEITSBERICHTE



4.1 Mitteilungen über Ausschlüsse vom Wahlrecht

Zur Vorbereitung und Durchführung von Wahlen dürfen Wahlrechtsausschlüsse im Melderegister gespeichert werden. Der Umfang der Mitteilungen für diese Zwecke entsprach in der Praxis nicht immer den datenschutzrechtlichen Vorgaben. Darüber hinaus führten fehlende Folgemitteilungen zu einer Reihe von Schwierigkeiten, unter anderem zu einer erheblichen Beeinträchtigung der Rechte der Betroffenen (siehe Vierter Tätigkeitsbericht, Punkt 3.1.12).

Mittlerweile haben die Justizverwaltungen der Länder die Anordnung über Mitteilungen in Strafsachen geändert, so dass für das Wählerverzeichnis nunmehr auch der später errechnete Zeitpunkt der Wiedererlangung der Amtsfähigkeit, der Wählbarkeit sowie des Wahl- und Stimmrechts oder die Wiedererteilung dieser Fähigkeiten und Rechte mitzuteilen sind. Diese Folgemitteilungen führen zu einer erfreulichen datenschutzrechtlichen Verbesserung. Sie gewährleisten, dass Wahlrechtsausschlüsse nur noch so lange gespeichert werden, wie sie auch tatsächlich bestehen.

4.2 Elektronisches Grundbuch

Über meine Beratungen bei der Einführung des elektronischen Grundbuches habe ich bereits in den vergangenen Jahren informiert (siehe Dritter Tätigkeitsbericht, Punkt 3.1.7; Vierter Tätigkeitsbericht, Punkt 3.1.8).

Nach wie vor ist nicht geklärt, wie die Auftragsdatenverarbeitung im Teilprojekt „Elektronische Unterschrift“ ausgestaltet werden soll, um den in § 126 Abs. 3 Grundbuchordnung vorgesehenen Grenzen zu entsprechen. Das Justizministerium hat hierzu mitgeteilt, dass aufgrund dieser restriktiven Regelung nur eine „verwaltungshelfende Einbindung“ der DVZ M-V GmbH möglich wäre. Deshalb wird in Erwägung gezogen, auf eine Änderung der Vorschrift hinzuwirken. Dieses Anliegen wird von mir unterstützt.

Die Entwicklung dieses recht umfangreichen Projektes werde ich auch weiterhin datenschutzrechtlich begleiten.

4.3 Wenn der Staatsanwalt zu Hause arbeitet

Staatsanwälte bearbeiten Verfahrensakte auch zu Hause und fertigen hierbei Schriftsätze am privaten Computer. Deshalb hatte ich vor einiger Zeit angeregt, in die Musterdienstanweisung zum Datenschutz auch Regelungen für den Umgang mit personenbezogenen Daten im häuslichen Bereich aufzunehmen (siehe Vierter Tätigkeitsbericht, Punkt 3.1.7).

Das Justizministerium beabsichtigt, für die Justizbehörden des Landes eine neue umfassende Musterdienstanweisung zum Datenschutz auf der Basis eines Rahmensicherheitskonzeptes zu erarbeiten. Bereits vorab wurden Regelungen zum Einsatz von privaten IT-Geräten bei der Verarbeitung dienstlicher Daten im häuslichen Bereich getroffen. Unter anderem wurde festgelegt, dass die Beschäftigten verpflichtet sind,

- personenbezogene Daten nur in anonymisierter oder pseudonymisierter Form automatisiert zu verarbeiten,
- Disketten mit dienstlichen Daten nicht privat zu entsorgen,
- dienstliche Daten im privaten Bereich vor dem Zugriff Dritter zu schützen, insbesondere Akten und Disketten mit dienstlichen Daten zu verschließen und getrennt von privaten Datenträgern aufzubewahren,
- Disketten zwischen dem Privat- und dem Dienstrechner nur persönlich zu transportieren und
- Daten von privaten Rechnern in den dienstlichen Bereich nur über eine „Datenschleuse“ zu übernehmen.

Diese Regelungen tragen dazu bei, den Anwender beim Umgang mit personenbezogenen Daten im privaten Bereich zu sensibilisieren und die Sicherheit der Daten zu erhöhen. Ich gehe davon aus, dass diese Festlegungen auch in die zu überarbeitende Musterdienstanweisung einfließen werden.

4.4 Ausübung des gemeindlichen Vorkaufsrechts

Bevor das Grundbuchamt den Kauf eines Grundstückes im Grundbuch einträgt, hat der Käufer unter anderem nachzuweisen, dass für dieses Grundstück kein gemeindliches Vorkaufsrecht besteht. Zu diesem Zweck sind Grundstückskäufe regelmäßig der Gemeinde anzuzeigen. Sie prüft, ob ein Vorkaufsrecht besteht und ob sie dieses wahrnehmen will. Macht die Gemeinde von ihrem Vorkaufsrecht keinen Gebrauch oder besteht ein solches Recht nicht, so erteilt sie zur Vorlage beim Grundbuchamt ein Negativattest gemäß § 28 Abs. 1 Baugesetzbuch (BauGB). Unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes und der datenschutzrechtlichen Belange der Vertragsparteien bei Grundstückskaufverträgen einerseits sowie des berechtigten Informationsinteresses der Gemeinden andererseits hatte ich empfohlen, für diese Prüfung ein zweistufiges Verfahren zu nutzen. In einem ersten Schritt erhält die Gemeinde lediglich eine Veräußerungsanzeige mit allen Daten, die für die Feststellung, ob für dieses Grundstück ein gemeindliches Vorkaufsrecht besteht, erforderlich sind. Nur in den Fällen, in denen ein Vorkaufsrecht existiert, übersendet der Notar in einem zweiten Schritt den vollständigen Kaufvertrag (siehe Dritter Tätigkeitsbericht, Punkt 3.7.2).

Im Frühjahr 2000 hat das Innenministerium eine mit dem Städte- und Gemeindetag, dem Landkreistag, dem Ministerium für Arbeit und Bau, der Notarkammer des Landes und meiner Behörde abgestimmte Anwendungsempfehlung für eine zweistufige Verfahrensweise bei der Beantragung von Negativattesten nach § 28 Abs. 1 BauGB und § 22 Abs. 3 Denkmalschutzgesetz des Landes Mecklenburg-Vorpommern herausgegeben. Soweit in Einzelfällen mit Einwilligung der Vertragsparteien hiervon abgewichen und der Gemeinde sofort der volle Inhalt des Vertrages mitgeteilt wird, ist ein entsprechender Vermerk in die Urkunde aufzunehmen oder die Einwilligung in sonstiger Weise zu dokumentieren.

Durch das zweistufige Verfahren wird den datenschutzrechtlichen Belangen der Vertragsparteien hinreichend Rechnung getragen.

4.5 Data Warehouse

Die Risiken bei der Verarbeitung personenbezogener Daten in einem Data Warehouse (DWH) habe ich bereits in meinem Vierten Tätigkeitsbericht unter Punkt 3.16.5 ausführlich dargestellt. Im Hinblick auf die zunehmende Verbreitung von Datenverarbeitungen nach dem DWH-Konzept hat die 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 2000 eine Entschließung verabschiedet,

in der sie einzelne Gefahren der DWH-Verfahren aufführt und die Rahmenbedingungen für ihren Einsatz darstellt (siehe Anlage 2).

Da zunehmend auch öffentliche Stellen Interesse an dem DWH-Konzept zeigen, habe ich zusammen mit dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg ein Arbeitspapier dazu erstellt. In ihm werden die rechtlichen Möglichkeiten des Einsatzes von DWH-Verfahren im öffentlichen Bereich erörtert und Vorschläge zur Anwendung verschiedener datenschutzfreundlicher Technologien unterbreitet. Die wichtigsten Ergebnisse sind:

- Für das Betreiben eines DWH mit personenbezogenen Daten existiert derzeit keine Rechtsgrundlage.
- Unter Nutzung datenschutzfreundlicher Technologien können DWH-Systeme so konzipiert werden, dass sie den allgemeinen datenschutzrechtlichen Anforderungen genügen.
- Strategische Informationen im Bereich der Verwaltung können auch gewonnen werden, indem der Personenbezug von Einzelangaben entfernt wird und diese dann nach bestimmten Kriterien zusammengefasst und anschließend neu aufgeteilt werden (Aggregation und Partitionierung).

Das Arbeitspapier ist kostenlos bei mir erhältlich.

Nach Auskunft des interministeriellen Ausschusses für Informations- und Telekommunikationstechnik (IMA-IT) sind in Mecklenburg-Vorpommern keine Landesverfahren geplant, die bei der Verarbeitung personenbezogener Daten DWH-Techniken verwenden.

4.6 Volkszählung

Die nächste Volkszählung (Zensus) in Deutschland wird hauptsächlich auf der Auswertung von Verwaltungsregistern und nicht mehr auf einer Bevölkerungsbefragung beruhen. Dazu müssen Testerhebungen durchgeführt werden, die in einem speziellen Gesetz zu regeln sind (siehe Vierter Tätigkeitsbericht, Punkt 3.7).

Am 27. Juli 2001 wurde das Zensusvorbereitungsgesetz mit dem Zensusertestgesetz verabschiedet (BGBl. I S. 1882). Das Zensusertestgesetz ordnet verschiedene Testerhebungen auf Stichprobenbasis an und legt die Verfahren zur Verarbeitung der ge-

wonnenen Daten fest. Erhebungen werden bei den Meldebehörden, bei Bewohnern und Eigentümern bestimmter Gebäude in ausgewählten Gemeinden sowie bei der Bundesanstalt für Arbeit durchgeführt. Der Datenkatalog ist gegenüber einem „echten“ Zensus deutlich reduziert, da nur die Daten erfragt werden, die erforderlich sind, um die Zensustauglichkeit der Register zu prüfen. Erhebungsmerkmale bei der Befragung der Gebäudebewohner sind beispielsweise Geburtsmonat und -jahr, Geschlecht, Familienstand und Wohnort, Hilfsmerkmale sind Namen, Anschriften, Geburtsdaten, Angaben zu Umzügen sowie An- und Abmeldungen bei den Meldebehörden. Einkommensangaben oder ähnlich sensible Daten werden nicht erhoben.

Die aus den verschiedenen Erhebungen gewonnenen Daten werden ausschließlich bei den Statistikämtern der Länder oder beim Statistischen Bundesamt zusammengeführt und abgeglichen. Sie unterliegen der statistischen Geheimhaltung. Eine Weitergabe und Verwendung der Daten zu Verwaltungszwecken ist ausgeschlossen. Insbesondere bei Unklarheiten von Angaben aus den Melderegistern wird nicht bei den Meldeämtern nachgefragt, sondern nur bei den betroffenen Einwohnern. Vor- und Nachnamen sowie die meisten sonstigen Hilfsmerkmale werden bis spätestens Ende März 2004 gelöscht.

Am 5. Dezember 2001 hat die Befragung der Bewohner und Eigentümer der durch die Stichprobe bestimmten Gebäude begonnen. In Mecklenburg-Vorpommern sind dies 2.348 Gebäude in 39 Gemeinden. Die Bewohner werden durch geschulte Interviewer des Statistischen Landesamtes und die Eigentümer auf postalischem Weg befragt. Die Bewohner können die Daten dem Interviewer mitteilen oder die ausgefüllten Fragebögen dem Statistischen Landesamt zusenden. Ausführliche Informationen zum Zensustest sind beim Statistischen Landesamt, Postfach 12 01 35, 19018 Schwerin, erhältlich oder können auf dessen Homepage im Internet unter www.statistik-mv.de abgerufen werden.

4.7 Öffentliche Auslegung von Wählerverzeichnissen

Vor Wahlen werden die Wählerverzeichnisse ausgelegt, damit die Bürger kontrollieren können, ob sie richtig und vollständig sind. Obwohl die Meldebehörde keine Auskunft über Einwohner erteilen darf, für die eine melderechtliche Auskunftssperre besteht, kann jedermann Namen und Adresse dieser Einwohner durch Einsicht in ein öffentlich ausgelegtes Wählerverzeichnis zur Kenntnis nehmen. Die Datenschutzbeauftragten des Bundes und der Länder haben sich schon 1995 in einer Entschließung gegen dieses Verfahren ausgesprochen. Auch das Innenministerium unseres Landes hält diese Offenlegung für nicht datenschutzgerecht, lehnte eine Änderung

aber bisher ab, da in Mecklenburg-Vorpommern meist verschiedene Wahlen – beispielsweise Landtags- und Bundestagswahlen – gemeinsam stattfinden und das Bundeswahlgesetz ebenfalls eine öffentliche Auslegung des Wählerverzeichnisses vorsieht (siehe Zweiter Tätigkeitsbericht, Punkt 2.10.1 und Anlage 17).

Im April 2001 wurde das Bundeswahlgesetz novelliert und enthält nun in § 17 Abs. 1 Satz 3 und 4 folgende Bestimmungen:

„Zur Überprüfung der Richtigkeit oder Vollständigkeit der Daten von anderen im Wählerverzeichnis eingetragenen Personen haben Wahlberechtigte (...) nur dann ein Recht auf Einsicht in das Wählerverzeichnis, wenn sie Tatsachen glaubhaft machen, aus denen sich eine Unrichtigkeit oder Unvollständigkeit des Wählerverzeichnisses ergeben kann. Das Recht zur Überprüfung (...) besteht nicht hinsichtlich der Daten von Wahlberechtigten, für die im Melderegister ein Sperrvermerk (...) eingetragen ist.“

Diese datenschutzfreundlichen Regelungen wurden im September 2001 wörtlich in den § 18 Abs. 1 des Landeswahlgesetzes übernommen. Nach Auskunft des Innenministeriums soll das Kommunalwahlgesetz demnächst entsprechend geändert werden. Auch in Mecklenburg-Vorpommern werden Wählerverzeichnisse dann künftig nicht mehr öffentlich ausgelegt werden.

4.8 INPOL-neu

Im Rahmen der Neukonzeption des polizeilichen Informationssystems (INPOL) war geplant, neben bundesweit verfügbaren Verbunddaten auch Landesbestände im Wege der Auftragsdatenverarbeitung logisch getrennt in der INPOL-Datenbank zu speichern. Zudem sollten aufgrund bilateraler Absprachen landesspezifische Informationen in bestimmtem Umfang gespeichert und gegenseitige Zugriffe einzelner Länder auf die Datenbestände ermöglicht werden (siehe Erster Tätigkeitsbericht, Punkt 2.4.2; Zweiter Tätigkeitsbericht, Punkt 2.3.2; Vierter Tätigkeitsbericht, Punkt 3.2.1).

Die Datenschutzbeauftragten des Bundes und der Länder hatten eine dauerhafte Speicherung von Landesdaten beim Bundeskriminalamt kritisiert, da dies die Trennung von Landesdaten und Verbunddaten aufweichen würde (zu den Einzelheiten siehe Entschließung der 60. Konferenz vom 12./13. Oktober 2000, Anlage 7). Aus Kostengründen haben sich jedoch viele Länder, so auch Mecklenburg-Vorpommern, für eine Auftragsdatenverarbeitung beim Bundeskriminalamt entschieden. Im September 2001 teilte unser Innenministerium mit, dass entsprechende Vertragsgewürfe

noch einmal überarbeitet werden würden. Kurze Zeit später konnte ich der Presse entnehmen, dass das gesamte Projekt INPOL-neu wegen erheblicher Mängel vorerst gestoppt worden ist.

Bis zum Redaktionsschluss habe ich keine Mitteilung zum aktuellen Sachstand aus dem Innenministerium erhalten.

4.9 Novellierung des Sicherheits- und Ordnungsgesetzes (SOG M-V)

Unter der Überschrift „Verfassungsgericht stoppt Schleierfahndung“ hatte ich bereits in meinem Vierten Tätigkeitsbericht, Punkt 3.2.2, berichtet, dass das Landesverfassungsgericht die Bestimmungen des SOG zu verdachts- und ereignisunabhängigen Personenkontrollen als überwiegend verfassungswidrig erklärt hat. In einer weiteren Entscheidung hat das Gericht im Mai 2000 die Regelungen, die die polizeiliche Überwachung von Wohnungen und Datenerhebungen aus dem Bereich geschützter Vertrauensverhältnisse erlauben, ebenfalls als überwiegend verfassungswidrig erklärt.

Die daraufhin erforderlichen Korrekturen wurden mit dem Zweiten Gesetz zur Änderung des Sicherheits- und Ordnungsgesetzes realisiert, das am 24. Oktober 2001 vom Landtag verabschiedet worden ist.

Das neue Gesetz erlaubt an Stelle der verdachts- und ereignisunabhängigen Personenkontrollen nunmehr so genannte Anhalte- und Sichtkontrollen. Die Polizei darf unter bestimmten Voraussetzungen eine Person kurzfristig anhalten und das mitgeführte Fahrzeug in Augenschein nehmen. Laut Gesetzesbegründung braucht die betroffene Person weder ihre Identität preiszugeben noch Ausweispapiere vorzulegen. In dem nachfolgenden Paragraphen (§ 28) ist jedoch geregelt, dass eine Person ohne das Vorliegen besonderer Voraussetzungen auf Befragen hin auch Namen, Vornamen, Tag und Ort der Geburt, Wohnanschrift und Staatsangehörigkeit anzugeben, mit anderen Worten ihre Identität preiszugeben hat. Aufgrund der Inkonsistenz dieser Vorschriften bleibt unklar, unter welchen Voraussetzungen sich der Bürger auszuweisen hat. Des Weiteren ist es bedenklich, wenn er als unbescholtener Bürger ohne Anlass eine Inaugenscheinnahme seines Fahrzeuges einschließlich Kofferraum samt Inhalt hinnehmen muss. Aus datenschutzrechtlicher Sicht fehlt an dieser Stelle die unentbehrliche Abgrenzung zu weitergehenden Eingriffsbefugnissen.

Neu geregelt ist auch der so genannte Große Lauschangriff. Danach sind Datenerhebungen mit technischen Mitteln aus Wohnungen sowie aus geschützten Vertrauensverhältnissen nur noch möglich, sofern eine gegenwärtige Gefahr für Leib, Leben

oder Freiheit einer Person abzuwehren ist. Damit ist der Gesetzgeber den Forderungen des Landesverfassungsgerichtes gefolgt. Allerdings wurde nicht hinreichend klar gestellt, wer alles zum Kreis der betroffenen Personen gehört, die in eine verdeckte Maßnahme einbezogen sind.

Auch zu Datenübermittlungen an andere Behörden oder Stellen enthält das novelierte Gesetz neue Regelungen. Es erlaubt nunmehr, Polizeidaten an private Stellen zu übermitteln, soweit sie an der „Abwehr von Gefahren“ beteiligt sind. Bisher sah das Sicherheits- und Ordnungsgesetz ein abgestuftes Verhältnis zwischen Datenübermittlungen aus dem Polizeibereich an öffentliche Stellen einerseits und an Personen oder Stellen außerhalb des öffentlichen Bereichs andererseits vor. Diese Unterscheidung wurde nunmehr aufgehoben. Es ist der Polizei jetzt möglich, sensible Polizeidaten beispielsweise an private Sicherheitsdienste oder in Fällen häuslicher Gewalt an private Interventionsstellen zu übermitteln, ohne vorher das Einverständnis der Betroffenen einzuholen. Nicht die Betroffenen selbst, sondern die Polizei bestimmt, ob und in welchem Umfang sie Daten weitergibt. Das Gesetz geht in diesem Punkt weit über die Regelungen der Polizeigesetze anderer Länder hinaus.

4.10 Die neue Telekommunikations-Datenschutzverordnung

Am 21. Dezember 2000 ist die Telekommunikations-Datenschutzverordnung (TDSV) in Kraft getreten. Sie löste die Telekommunikationsdienstunternehmen-Datenschutzverordnung aus dem Jahre 1996 ab.

Die Gründe für die Schaffung der neuen TDSV und meine Empfehlungen zur Verbesserung des Entwurfes vom 21. Oktober 1999 sind im Vierten Tätigkeitsbericht unter Punkt 3.8.1 dargestellt. Der Text dieses Entwurfes wurde vor In-Kraft-Treten der Verordnung nur noch unwesentlich geändert. Die neue Verordnung enthält somit gegenüber der von 1996 zwar datenschutzrechtliche Verbesserungen; die meisten Bedenken und Empfehlungen blieben jedoch unberücksichtigt. Auch die neue TDSV weist damit Regelungen auf, die die Rechte Betroffener unverhältnismäßig einschränken.

Ein Beispiel für eine datenschutz- und auch verbraucherunfreundliche Regelung ist die Vorschrift zur Entgeltermittlung und -abrechnung. Danach können die TK-Unternehmen Verbindungsdaten ihrer Kunden statt bisher 80 Tage nun sogar sechs Monate lang nach Versenden der Rechnung speichern. Diese Datenspeicherung auf Vorrat dient nicht der Abwicklung des TK-Verkehrs, sondern eventuell künftigen Zugriffen der Sicherheitsbehörden. Der Betroffene kann die Speicherung nur verhindern, indem

er von dem TK-Dienstleister die Löschung seiner Verbindungsdaten unmittelbar nach Rechnungsversand verlangt. Die rechnungsstellenden TK-Unternehmen sind dann nach der TDSV zur Löschung dieser Daten verpflichtet, können sie dann aber im Fall eines Rechtsstreits um die angefallenen Telefongebühren nicht mehr vorlegen. TK-Dienstleister, von denen der Kunde keine Rechnung erhält, beispielsweise Anbieter von Call-by-Call-Dienstleistungen, sind nicht zur Löschung verpflichtet. Hier kann der Kunde die Löschung seiner Daten nur erreichen, wenn er sich von jedem Anbieter eine eigene Rechnung stellen lässt.

Im Jahr 2002 wird voraussichtlich die EG-Telekommunikations-Datenschutzrichtlinie novelliert. Es bleibt zu hoffen, dass im Zuge der Anpassung der TDSV an diese Richtlinie wenigstens einige der Einschränkungen des Rechts auf informationelle Selbstbestimmung beseitigt werden.

5.

ARBEITSKREIS „TECHNISCHE UND ORGANISATORISCHE DATENSCHUTZFRAGEN“ (AK TECHNIK)

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ ist ein Gremium der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, in dem die Techniker aller Dienststellen zusammenarbeiten. Seine Hauptaufgabe ist die Beratung der Konferenz zu technischen Fragen. Im Berichtszeitraum wurden Entschlüssen der Konferenz zu den Themen Data Warehouse (siehe Punkt 4.5) und Straßenbenutzungsgebühren (siehe Punkt 3.4.3) vorbereitet. Darüber hinaus erstellten die Mitglieder im Auftrag der Konferenz ein Arbeitspapier zum Thema transparente Software (siehe Punkt 3.18.6), in dem das Open-Source-Modell aus datenschutztechnischer Sicht bewertet wird.

Aber auch bei technischen Fragen zur Organisation der eigenen Dienststellen berät der Arbeitskreis. So wurden die technischen und organisatorischen Rahmenbedingungen und die notwendigen Einführungsstrategien erarbeitet, damit die Datenschutzbeauftragten bei Bedarf untereinander verschlüsselt per E-Mail kommunizieren können.

Als Vorsitzender des Arbeitskreises habe ich in den vergangenen zwei Jahren vier Sitzungen in Schwerin, Rostock und Regensburg organisiert. Die Tagungsorte standen im Zusammenhang mit den jeweiligen Schwerpunktthemen, die beraten wurden. So tagte der Arbeitskreis im Herbst 2000 auf Einladung des Fachbereiches Informatik an der Universität in Rostock. Wissenschaftler des Fachbereiches stellten Forschungsprojekte vor, um den Stand der Technik beispielsweise im Bereich der Kryptographie, der Chipkartentechnik oder der mobilen Informationstechnik zu demonstrieren, und nutzten die Gelegenheit, die datenschutztechnischen Aspekte verschiedener Projekte mit den Mitgliedern des Arbeitskreises zu diskutieren. Es wurde vereinbart, künftig in zunehmendem Maße bei Projekten mit datenschutzrechtlichem Bezug zusammenzuarbeiten.

Im Januar 2001 hatte das Universitätsklinikum Regensburg den Arbeitskreis eingeladen, um datenschutztechnische Fragen beim Einsatz von Informations- und Kommunikationstechnik in der Medizin zu beraten. Die Mediziner des Klinikums stellten EDV-Projekte aus verschiedenen Bereichen der Telemedizin (beispielsweise Teleradiologie, Teledermatologie) vor und diskutierten mit den Arbeitskreismitgliedern unter anderem Aspekte der Pseudonymisierung von Patientendaten und der Vernetzung von medizinischen Einrichtungen. Im Ergebnis dieser Sitzung wurde eine Arbeitsgruppe gebildet, die konkrete Empfehlungen zur datenschutzgerechten Ausgestaltung medizinischer Informationssysteme erarbeiten soll.

Die Nutzung des Internet durch öffentliche Stellen ist zu einem Dauerthema im Arbeitskreis geworden. Bereits 1995 gab der Arbeitskreis die erste Orientierungshilfe

zum Thema Internet heraus (siehe Zweiter Tätigkeitsbericht, Punkt 2.21). Wegen der sich rasant entwickelnden Technik war eine Überarbeitung bald erforderlich. Im September 1998 legte der Arbeitskreis eine zweite, aktualisierte Auflage vor (siehe Vierter Tätigkeitsbericht, Punkt 4). Um neben den technischen Entwicklungen auch einige rechtliche Aspekte aufnehmen zu können, wurde der Arbeitskreis „Medien“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gebeten, sich an einer erneut anstehenden Aktualisierung zu beteiligen. Im November 2000 war dann die dritte Auflage fertiggestellt. Sie wurde gemeinsam mit der Orientierungshilfe „Verzeichnisdienste“ (siehe Punkt 3.17.5) und Hinweisen zur Präsentation von Behörden im Internet in einer Broschüre „Datenschutz bei der Nutzung von Internet und Intranet“ veröffentlicht. Wie groß der Bedarf an Informationen zu diesem Themenkomplex ist, zeigt die Tatsache, dass die gesamte Auflage dieser Broschüre (5000 Exemplare) in kürzester Zeit vergriffen war. Um der schnellen Entwicklung im Bereich des Internet angemessen Rechnung tragen zu können und Publikationskosten zu sparen, ist vorgesehen, derartige Informationsmaterialien künftig vorwiegend im gemeinsamen Internetangebot der Datenschutzbeauftragten des Bundes und der Länder (www.datenschutz.de) zu veröffentlichen. Alle Publikationen des Arbeitskreises stehen auch in meinem Internetangebot (siehe Punkt 6) zum Abruf bereit.

6. ÖFFENTLICHKEITSARBEIT

Das Interesse an aktuellen Fragen des Datenschutzes hat in den vergangenen zwei Jahren bei den Bürgerinnen und Bürgern sowie bei den öffentlichen Stellen des Landes weiter zugenommen. Das spiegelte sich auch wider am „Tag der offenen Tür des Landtages“ und beim „Mecklenburg-Vorpommern-Tag“ in Greifswald, wo viele Gäste die Gelegenheit zum persönlichen Gespräch wahrnahmen.

Viele Institutionen haben mich gebeten, in Vorträgen und anderen Veranstaltungen zum Datenschutz zu informieren. Von besonderem Interesse waren dabei neben den datenschutzrechtlichen Grundlagen verschiedene Aspekte der Videoüberwachung, Fragestellungen aus dem Bereich des Patienten- und Sozialdatenschutzes sowie der Telemedizin und datenschutztechnische Aspekte der Telearbeit, der Internetnutzung, der Vernetzung, der Telekommunikation und der Revision.

Besonders erfreulich ist die Tatsache, dass bei der Hoch- und Fachschulausbildung von Juristen, Informatikern und Verwaltungsfachleuten immer öfter Datenschutzthemen berücksichtigt werden. In den Fachbereichen Informatik der Universität Rostock sowie Wirtschaft, Elektrotechnik und Informatik der Hochschule Wismar halten meine Mitarbeiter seit einiger Zeit regelmäßig Vorlesungen und führen Seminare insbesondere zu datenschutztechnischen Fragestellungen durch. Auch bei den jährlich stattfindenden Wirtschaftsinformatik-Tagen der Wismarer Hochschule ist meine Dienststelle regelmäßig mit Fachvorträgen vertreten. Mit angehenden Juristen der Ernst-Moritz-Arndt-Universität Greifswald wurden im Rahmen eines Fachseminars technische und rechtliche Aspekte der Videoüberwachung diskutiert. Auch die Fachhochschule für öffentliche Verwaltung und Rechtspflege in Güstrow hat Datenschutzthemen in ihr Fortbildungsprogramm aufgenommen. In zwei Seminaren haben meine Mitarbeiter Grundkenntnisse zu datenschutzrechtlichen und -technischen Fragen vermittelt. Des Weiteren haben sie beim IT-Forum Mecklenburg-Vorpommern, das regelmäßig an der Fachhochschule durchgeführt wird, Workshops durchgeführt und Vorträge gehalten.

Darüber hinaus ergaben sich noch weitere Möglichkeiten, die Aus- und Weiterbildung insbesondere im technischen Bereich zu unterstützen. Im Berichtszeitraum haben beispielsweise zwei Informatikstudenten der Hochschule Wismar mein Angebot angenommen, ihre Diplomarbeit zu datenschutzrelevanten Themen zu schreiben. Weiterhin konnten zwei Umschüler im Rahmen ihrer Ausbildung zum IT-Kaufmann erfolgreich ein dreimonatiges Praktikum in meiner Dienststelle absolvieren.

Der Bedarf an schriftlichem Informationsmaterial ist nach wie vor groß (Gesamtübersicht der Publikationen siehe Punkt 10). Die Loseblattsammlung „Gesetze und Verordnungen zum Datenschutz“ ist Ende 2001 erneut vollständig überarbeitet wor-

den. Erstellt wurden die Orientierungshilfen „Telearbeit“ (siehe Punkt 3.18.3) und „Präsentation von öffentlichen Stellen im Internet“ (siehe Punkt 3.17.4). Neben diesen Unterlagen sind auch alle Arbeitsmaterialien des Arbeitskreises “Technische und organisatorische Datenschutzfragen” (siehe Punkt 5) in meiner Dienststelle kostenlos erhältlich.

Zu einer wichtigen Informationsquelle für Bürger und Behörden hat sich das Internetangebot meiner Dienststelle entwickelt. Alle in Papierform vorhandenen Materialien stehen unter www.lfd.m-v.de zum Abruf bereit. Darüber hinaus sind dort Links zu den Angeboten meiner Kollegen vom Bund und aus den Ländern zu finden. Informationen können seit Ende 2000 auch über das so genannte Virtuelle Datenschutzbüro (www.datenschutz.de) erschlossen werden. Das Virtuelle Datenschutzbüro ist ein Angebot von deutschen und ausländischen Datenschützern im Internet. Es bietet Informationen rund um den Datenschutz, Diskussionsforen zu aktuellen Datenschutzthemen, und es ist eine Plattform für die Zusammenarbeit der Datenschützer.

7

ANLAGEN



1. Anlage: Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Konsequenzen aus dem Urteil des Bundesverfassungsgerichtes zu den Abhörmaßnahmen des BND

Das Bundesverfassungsgericht hat für die Verwendung von Daten, die aus der Fernmeldeüberwachung gewonnen wurden, deutliche Schranken gezogen, die weit über den Gegenstand des Verfahrens hinaus bedeutsam sind.

Das Gericht betont die Bedeutung des Fernmeldegeheimnisses zur Aufrechterhaltung einer freien Telekommunikation, die eine Grundvoraussetzung der Informationsgesellschaft darstellt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichtes zu den verdachtslosen Abhörmaßnahmen des BND auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird (Telefon, E-Mail, Telefax, Internet-Abrufe o. ä.).

Die Anforderungen des Urteils müssen auch Konsequenzen für Fallgestaltungen haben, bei denen personenbezogene Daten durch Maßnahmen erlangt werden, die in ihrer Art und Schwere einer Beschränkung des Fernmeldegeheimnisses gleichkommen, insbesondere etwa bei einer Erhebung durch Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes mit dem Einsatz technischer Mittel.

Die Anforderungen aus dem Urteil sind unverzüglich umzusetzen:

- Zur Sicherung der Zweckbindung der erlangten Daten und für die Kontrolle ihrer Verwendung muss ihre Herkunft aus Eingriffen in das Fernmeldegeheimnis oder vergleichbaren Eingriffen durch eine entsprechende Kennzeichnung nach der Erfassung auch bei den Übermittlungsempfängern erkennbar bleiben.
- Die erlangten Daten müssen bei allen speichernden Stellen unverzüglich gelöscht werden, wenn sie nicht mehr erforderlich sind – es sei denn, der Rechtsschutz der Betroffenen würde dadurch verkürzt. Die Praxis von Verfassungsschutzämtern, nicht (mehr) erforderliche Daten, wenn sie sich in Unterlagen befinden, nicht zu schwärzen, kann – zumindest bei Daten, die durch Eingriffe in das Fernmeldegeheimnis oder vergleichbare Eingriffe erlangt wurden – nicht mehr aufrechterhalten werden. Um die Notwendigkeit einer späteren Schwärzung zu vermeiden, sollte bereichsspezifischen Vernichtungsregelungen bereits bei der Aktenführung Rechnung getragen werden.

- Die Vernichtungspflicht ist im Licht von Art. 19 Abs. 4 GG zu verstehen. Danach sind Maßnahmen unzulässig, die darauf abzielen oder geeignet sind, den Rechtsschutz der Betroffenen zu vereiteln. Eine Löschung oder Vernichtung ist nach einem Auskunftsantrag bei allen personenbezogenen Daten unzulässig. Zudem sind personenbezogene Daten, die durch die o. g. Maßnahmen erlangt wurden, nach einer Unterrichtung der Betroffenen für einen angemessenen Zeitraum – ausschließlich zum Zweck der Sicherung des Rechtsschutzes – aufzubewahren.
- Überwachte Personen müssen von Eingriffen unterrichtet werden, sobald dadurch der Zweck der Maßnahme nicht mehr gefährdet wird; dies gilt auch für weitere Betroffene, es sei denn, überwiegende schutzwürdige Belange der überwachten Person stehen dem entgegen (Schutz vor unnötiger Bloßstellung). Wie bei Eingriffen in das Fernmeldegeheimnis ist dies auch bei anderen verdeckten Maßnahmen Voraussetzung dafür, dass die Betroffenen von den ihnen zustehenden Rechten Gebrauch machen können, und daher von Art. 19 Abs. 4 GG geboten. Speicherfristen können die Unterrichtungspflicht nicht beseitigen, irrelevante Daten sind umgehend zu löschen.
- Damit sind Regelungen z. B. in Landesverfassungsschutz- und Polizeigesetzen nicht zu vereinbaren, wonach eine Unterrichtung der Betroffenen über Datenerhebungen, die in ihrer Art und Schwere einem Eingriff in das Fernmeldegeheimnis gleichkommen, unterbleibt, wenn sich auch nach fünf Jahren nicht abschließend beurteilen lässt, ob eine Gefährdung des Zweckes des Eingriffes ausgeschlossen werden kann. Zusätzlich zur unbefristeten Benachrichtigungspflicht ist eine Mitteilung an die Datenschutzkontrollstelle für den Fall vorzusehen, dass die Unterrichtung der Betroffenen länger als fünf Jahre zurückgestellt wird.
- Der Umgang des Verfassungsschutzes mit personenbezogenen Daten, die in Durchbrechung des Fernmeldegeheimnisses erhoben worden sind, ist durch eine unabhängige Datenschutzkontrollstelle lückenlos zu überprüfen.
- Eine Kontrollücke bei personenbezogenen Daten, die durch G 10-Maßnahmen erlangt wurden, wäre verfassungswidrig. Das Bundesverfassungsgericht hat hervorgehoben, dass Art. 10 GG eine umfassende Kontrolle durch unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane gebietet.
- Die Kontrolle muss sich auf den gesamten Prozess der Erfassung und Verwertung der Daten einschließlich der Benachrichtigung – bei Datenübermittlungen auch bei den Datenempfängern – erstrecken.

- Der Gesetzgeber sollte festlegen, dass die Übermittlung der Daten, die Prüfung der Erforderlichkeit weiterer Speicherung sowie die Durchführung der Vernichtung und Löschung der Daten aus G 10-Maßnahmen zu protokollieren sind.
- Für eine effektive Kontrolle sind die zuständigen Stellen personell und sachlich angemessen auszustatten.
- Die Ausführungsgesetze zum G 10 müssen hinsichtlich der Kontrolle eindeutig sein. Es ist klarzustellen, inwieweit die G 10-Kommissionen auch für die Kontrolle der weitergehenden Datenverarbeitung zuständig sind oder inwieweit die Kontrolle von den Datenschutzbeauftragten wahrzunehmen ist.

2. Anlage: Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Data Warehouse, Data Mining und Datenschutz

Mit der ständig zunehmenden Leistungsfähigkeit der Informations- und Kommunikationstechnik wächst die Menge gespeicherter personenbezogener Daten in Wirtschaft und Verwaltung weiter an. Zunehmend kommen automatisierte Verfahren zum Einsatz, die das gesammelte Datenmaterial effektiv verwalten und analysieren. Im "Data Warehouse" werden alle verwendbaren Daten in einem einheitlichen Datenpool losgelöst von ihrer ursprünglichen Verwendung zusammengeführt. "Data Mining" bietet Werkzeuge, die die scheinbar zusammenhanglosen Daten nach noch nicht bekannten, wissenswerten Zusammenhängen durchsuchen, Daten aufspüren, kombinieren und neue Informationen zur Verfügung stellen.

Diese Entwicklung schafft neben Vorteilen neue Gefahren und Risiken für das Grundrecht auf informationelle Selbstbestimmung und für den Schutz der Privatheit: Persönlichkeitsprofile, automatisierte Vorhersagen von Verhaltens- und Handlungsweisen, Manipulationsmöglichkeiten und zu lange Speicherung sind befürchtete Gefahren.

Die Konferenz der Datenschutzbeauftragten weist auf Folgendes hin:

- Nach dem grundrechtlichen Gebot der Zweckbindung dürfen personenbezogene Daten nur im Rahmen der gesetzlich zugelassenen Zwecke oder der gegenseitigen Vereinbarungen verwendet werden. Eine personenbezogene Speicherung in einem allgemein verwendbaren Data Warehouse entfernt sich vom ursprünglichen Verwendungszweck und stellt eine Speicherung auf Vorrat ohne Zweckbindung dar. Personenbezogene Daten, die bei der öffentlichen Verwaltung vorhanden sind, sind in ihrer Zweckbestimmung grundrechtlich geschützt und dürfen nicht für unbestimmte Zwecke in einem "Daten-Lagerhaus" gesammelt werden.
- Eine Zweckänderung ist nur mit Einwilligung der Betroffenen zulässig, nachdem diese über die Tragweite der Einwilligung aufgeklärt worden ist. Eine Einwilligung in unbestimmte und zeitlich unbegrenzte Zweckänderungen ist deswegen unwirksam.

- Gestaltung und Auswahl von Datenverarbeitungs-Systemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Anonyme und pseudonyme Verfahren sind datenschutzrechtlich unbedenklich.
- Verfahren sind so zu gestalten, dass die Betroffenen hinreichend unterrichtet werden, damit sie jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen können. Sie haben insbesondere das Recht, eine erteilte Einwilligung jederzeit zurückzuziehen.
- Die gesetzlichen Speicherfristen, nach deren Ablauf die Daten zwingend archiviert oder gelöscht werden müssen, sind strikt zu beachten. Deswegen ist die Einrichtung von permanenten "Daten-Lagerhäusern" rechtswidrig.
- Die Europäische Datenschutzrichtlinie spricht grundsätzlich jeder Person das Recht zu, keiner belastenden automatisierten Einzelentscheidung unterworfen zu werden (Art. 15). "Data Mining" ist ein Instrument, das für solche Entscheidungen herangezogen werden kann.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ruft die Hersteller und Anwender von "Data Warehouse"- und "Data Mining"-Verfahren dazu auf, solchen Programmen den Vorzug zu geben, die unter Einsatz von datenschutzfreundlichen Technologien die Speicherung von personenbezogenen Daten durch Anonymisierung oder Pseudonymisierung vermeiden.

3. Anlage: Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Unzulässiger Speicherungsumfang in “INPOL-neu” geplant

Das Bundeskriminalamt und die Polizeien der Bundesländer konzipieren seit geraumer Zeit unter der Bezeichnung “INPOL-neu” eine Fortentwicklung des gemeinsamen Informationssystems. Inzwischen steht der Beginn der schrittweisen Einführung des neuen Datenaustauschsystems kurz bevor.

Das Informationssystem INPOL wirft in vielfacher Hinsicht datenschutzrechtliche Probleme auf. Die Datenschutzbeauftragten des Bundes und der Länder haben mehrfach aus konkretem Anlass darauf hingewiesen, dass nicht jede mit den heutigen technischen Möglichkeiten realisierbare oder mit polizeifachlicher Erforderlichkeit begründete Verarbeitung personenbezogener Daten zulässig ist. Bereits bei der Konzeption des INPOL-Systems muss vielmehr dafür Sorge getragen werden, dass in das Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung nur soweit eingegriffen wird, wie dies im Rahmen der Erforderlichkeit für die polizeiliche Aufgabenerfüllung durch Rechtsvorschriften erlaubt wird.

Es besteht jedoch Grund zu der Sorge, dass es bei der Neugestaltung des INPOL-Systems zu falschen Weichenstellungen mit der Folge unzulässiger Verarbeitung personenbezogener Daten kommt. Die zu befürchtende Fehlentwicklung liegt darin, dass das Bundeskriminalamt und die Landeskriminalämter planen, künftig im Bundes-Kriminalaktennachweis (KAN) die “gesamte kriminelle Karriere” jeder Person abzubilden, die aus Anlass eines INPOL-relevanten Delikts erfasst ist. Es sollen in diesen Fällen auch Daten über solche Straftaten gespeichert und zum Abruf bereit gehalten werden, die weder von länderübergreifender oder internationaler noch von besonderer Bedeutung sind.

§ 2 Abs. 1 BKAG beschränkt die Zuständigkeit des BKA (als Zentralstelle des polizeilichen Informationssystems) sowohl im präventiven als auch im repressiven Bereich auf “Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung”. Der Wortlaut ist eindeutig. Anknüpfungspunkt und Gegenstand der Einteilung in INPOL-relevante Informationen einerseits und INPOL-irrelevante Informationen andererseits sind die “Straftaten”, nicht die einzelne Person und auch nicht das “Gesamtbild einer Person”. Der Gesetzeswortlaut bildet die Grenze der Auslegung; eine über den Wortsinn hinausgehende Anwendung verstößt gegen das Gesetz. Daher ist es unzulässig, die Frage der INPOL-Relevanz unabhängig von der konkreten einzelnen Straftat zu beurteilen. Vielmehr dürfen im Bundes-KAN

nur Informationen zu solchen Straftaten verarbeitet werden, die im Einzelfall die in § 2 Abs. 1 BKAG aufgestellte Bedeutungsschwelle überschreiten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern das Bundesinnenministerium und die Innenministerien der Länder auf, von der geschilderten KAN-Erweiterung abzusehen.

4. Anlage: Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Strafverfahrensänderungsgesetz 1999 (StVÄG 1999)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen es, dass mit dem Entwurf für ein Strafverfahrensänderungsgesetz 1999 die Strafprozessordnung endlich die seit fast zwei Jahrzehnten überfälligen datenschutzrechtlichen Regelungen erhalten soll. Sie stellen jedoch fest, dass der nunmehr vorliegende Gesetzesbeschluss des Bundestages nicht alle wichtigen Forderungen des Datenschutzes erfüllt.

Darüber hinaus will der Bundesrat das Datenschutzniveau weiter absenken und hat auch zu diesem Zweck den Vermittlungsausschuss angerufen. Zu kritisieren ist, dass

- Zeuginnen und Zeugen auch bei Straftaten ohne erhebliche Bedeutung durch Öffentlichkeitsfahndung im Fernsehen oder Internet gesucht werden können,
- Zweckbindungen präventivpolizeilicher Daten, darunter auch der Erkenntnisse aus verdeckten Datenerhebungsmaßnahmen, wie z. B. einem Großen Lauschangriff oder einem Einsatz verdeckter Ermittler, völlig aufgehoben werden, so dass sie uneingeschränkt zur Strafverfolgung genutzt werden können,
- umgekehrt aber auch Informationen aus Strafverfahren über die Gefahrenabwehr hinaus uneingeschränkt zur Gefahrenvorsorge genutzt werden können,
- nicht am Verfahren beteiligte Dritte schon bei "berechtigtem Interesse" Einsicht in Strafverfahrensakten bekommen können.

Die Datenschutzbeauftragten des Bundes und der Länder sehen den verfassungsrechtlich gebotenen Ausgleich zwischen Persönlichkeitsschutz und Interessen der Strafverfolgungsbehörden nicht mehr als gewährleistet an, falls die Vorschläge des Bundesrates Eingang in die Strafprozessordnung finden sollten. Die Datenschutzbeauftragten fordern daher den Vermittlungsausschuss auf, die Änderungsanträge zurückzuweisen. Stattdessen sind Regelungen in der Strafprozessordnung vorzusehen, die geeignet sind, bei einer effektiven Strafverfolgung die Persönlichkeitsrechte der Betroffenen angemessen zu gewährleisten.

5. Anlage: Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Für eine freie Telekommunikation in einer freien Gesellschaft

Umfang und Intensität der Eingriffe in das von Art. 10 Grundgesetz geschützte Fernmeldegeheimnis haben in den letzten Jahren deutlich zugenommen. Ursächlich hierfür sind zum einen folgende Aspekte:

Erhebliche Zunahme der Telekommunikationsvorgänge

Die Zahl der Telekommunikationsvorgänge hat sich vervielfacht. Darüber hinaus werden neben dem traditionellen Telefon neue Kommunikationsmöglichkeiten wie Fax und PC-Fax, das Mobiltelefon, e-mail und mail-boxen sowie das Internet genutzt.

Stark angestiegener Umfang und wesentlich verbesserte Aussagequalität der Daten

Die digitale Datenverarbeitung ermöglicht detaillierte Auswertungen großer Datenmengen.

Die Datenverarbeitungsnetze bieten mehr und mehr aussagekräftige Bestandsdaten, wozu auch e-mail-Adresse, IP-Nummer oder domain name gehören. So können sich bei Mitgliedschaft in geschlossenen Netzen sogar Rückschlüsse auf Lebensanschauungen oder bestimmte Problemlagen ergeben, z. B. bei der Mitgliedschaft in bestimmten Interessengemeinschaften, etwa Aids-Selbsthilfegruppen.

Die Verbindungsdaten geben in der Regel Auskunft, wer wann mit wem wie lange und wie häufig kommuniziert hat; werden fremde Geräte verwendet, geraten Unbeteiligte in Verdacht.

Aus den Nutzungsdaten von Tele- und Mediendiensten lassen sich Rückschlüsse auf Interessengebiete und damit auf persönliche Eigenheiten und das Verhalten der Nutzenden ziehen.

Mobiltelefone ermöglichen schon im Stand-by-Modus die Bestimmung ihres Standorts.

Erleichterte Kenntnisnahme und Weiterverarbeitung dieser Daten

Die wesentlich erweiterten und einfacher nutzbaren technischen Möglichkeiten erlauben es, an verschiedenen Orten gespeicherte Daten zur Kenntnis zu nehmen und zu verarbeiten.

Entwicklung des Internet zum Massenkommunikationsmittel

Über das Netz werden immer mehr Alltagsgeschäfte abgewickelt: Wahrnehmung verschiedenartiger Informationsangebote, Erledigung von Bankgeschäften, Buchung von Reisen oder Bestellung von Waren und Dienstleistungen in virtuellen Kaufhäusern (e-commerce). Dadurch fallen immer mehr auswertbare Informationen über Lebensgewohnheiten und Bedürfnisse der Bürgerinnen und Bürger an.

Schwer durchschaubare Rechtslage

Die Zersplitterung der Regelungen in Strafprozess-, Telekommunikations- und Multimediarecht machen diese wenig transparent und schwer anwendbar.

Zum anderen ist dieser größere, leichter auswert- und verarbeitbare Datenpool wachsenden Zugriffswünschen der Sicherheitsbehörden im weitesten Sinn auf nationaler und internationaler Ebene ausgesetzt:

- Die Zahlen der Telekommunikations-Überwachungsanordnungen in den letzten Jahren sind kontinuierlich angestiegen: 1995: 3667, 1996: 6428, 1997: 7776, 1998: 9802
- Immer mehr Straftatbestände wurden als Grund für eine Telekommunikationsüberwachung in § 100 a der Strafprozessordnung (StPO) einbezogen – der Katalog wurde seit Einführung 11-mal erweitert und damit bis heute nahezu verdoppelt. Neue Erweiterungen sind im Gespräch.
- Die Telekommunikationsanbieter werden verpflichtet, technische Einrichtungen zur Umsetzung der Überwachungsanordnungen zu installieren und Kundendaten für Abfragen durch die Sicherheitsbehörden vorzuhalten zur Feststellung, mit welchen Anbietern verdächtige Personen einen Vertrag haben. Diese Verpflichtung wurde auch auf die Anbieter nicht gewerblicher Netze ausgedehnt und kann nach dem Gesetzeswortlaut auch Hotels, Betriebe, Behörden oder möglicherweise sogar Krankenhäuser betreffen.
- Ein europäischer Anforderungskatalog für Überwachungsmöglichkeiten unter dem Namen "ENFOPOL" befasst sich u. a. mit der Frage, welchen Anforde-

rungen die Netzbetreiber bzw. Diensteanbieter genügen müssen, damit die auf der Grundlage nationaler Ermächtigungsgrundlagen zulässige Telekommunikationsüberwachung technisch durchführbar ist. Die G8-Staaten haben noch weitergehende Beschlüsse gefasst.

Forderungen zur Gewährleistung der freien Telekommunikation

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits 1996 ein Positionspapier erarbeitet. Vor diesem Hintergrund fordert die Konferenz:

- Freie Telekommunikation ist unabdingbar für eine freiheitliche demokratische Kommunikationsgesellschaft. Sie wird durch das Fernmeldegeheimnis geschützt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichts zu den verdachtslosen Abhörmaßnahmen des BND (BVerfG, Urt. v. 14.7.1999, 1 BvR 2226/94 u. a.) auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird. Die Geltung des Fernmeldegeheimnisses ist deshalb auch für den Bereich der Tele- und Mediendienste ausdrücklich klarzustellen.
- Notwendig ist eine bürgerrechtsfreundliche technische Infrastruktur nach dem Grundsatz der Datenvermeidung und dem Datensparsamkeitsprinzip. Dabei ist der Einsatz datenschutzfreundlicher Technologien besonders zu fördern. Anonyme und pseudonyme Nutzungsmöglichkeiten müssen nach dem Vorbild des Teledienstedatenschutzgesetzes als Pflichtangebote vorgehalten werden. Die Nutzung dieser Angebote darf nicht von der Speicherung von Bestandsdaten abhängig gemacht werden. Eine Vorratshaltung von Daten Unverdächtiger über den Betriebszweck hinaus zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer zukünftiger Straftaten ist als Überwachung auf Vorrat abzulehnen.
- Notwendig ist deshalb ein zusammenfassendes, in sich schlüssiges System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf eine unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt.
- Als Grundlage hierfür ist eine Evaluierung der bestehenden Eingriffsregelungen nach objektiven, nicht zielorientierten Maßstäben vorzunehmen hinsichtlich Effektivität auf der einen und Eingriffsumfang auf der anderen Seite. Eine gesetzliche Berichtspflicht über Anlass, Verlauf, Ergebnisse und Anzahl der Betrof-

fenen ist auch für Telekommunikationsüberwachungen einzuführen. Dass auch Unverdächtige von Abhör- und Kontrollmaßnahmen betroffen sein können, ist dabei besonders zu berücksichtigen.

- Der aus der Frühzeit der analogen Fernsprechtechnik stammende § 12 Fernmeldeanlagen-gesetz, der die Herausgabe von Verbindungsdaten vergangener, nach bestrittener Rechtsprechung sogar zukünftiger Telekommunikationsvorgänge ohne Beschränkung auf schwerere Straftaten ermöglicht, muss wegen der erheblich höheren Aussagefähigkeit der digitalen Verbindungsdaten und des damit verbundenen Eingriffs in das Fernmeldegeheimnis zügig durch eine weniger weit reichende Regelung in der StPO ersetzt werden.
- Die Anforderungen aus dem bereits zitierten Urteil des Bundesverfassungsgerichts zur Telekommunikationsüberwachung sind unverzüglich umzusetzen.
- Die Ausweitung der Mitwirkungspflichten bei Überwachungsmaßnahmen auf Nebenstellenanlagen in Hotels, Krankenhäusern oder Betrieben wäre unverhältnismäßig. Es muss deshalb verbindlich klargestellt werden, dass die Betreiber dieser Nebenstellenanlagen nicht zur Bereitstellung entsprechender technischer Einrichtungen verpflichtet werden. Das Eckpunktepapier des Bundesministeriums für Wirtschaft und Technologie, das als Grundlage für einen Entwurf der Telekommunikations-Überwachungsverordnung dient und nach verschiedenen Gruppen von Betreibern differenziert, ist dazu ein erster Schritt. Auch muss möglichst durch eine Gesetzesänderung verhindert werden, dass die Verpflichtung, Kundendateien zu führen, auch für die o. g. Nebenstellenanlagen gilt. Darüber hinaus dürfen Anbieter von Guthabekarten zur Mobiltelefonie nicht dazu verpflichtet werden, Identifikationsdaten ihrer Kunden, die sie für betriebliche Zwecke nicht benötigen, ausschließlich für Zwecke der Strafverfolgungsbehörden und der Nachrichtendienste zu erheben und zum Abruf bereitzuhalten.
- Die Beachtung des Fernmeldegeheimnisses erfordert zwingend die Verschlüsselung von elektronischen Mitteilungen in offenen Netzen. Das Eckpunktepapier der Bundesregierung zur deutschen Kryptopolitik, das eine Kryptoregulierung ablehnt, ist ein wichtiger Schritt in die richtige Richtung. Gewerbliche Telekommunikationsdienstleister sollten gesetzlich verpflichtet werden, die Möglichkeit der verschlüsselten Kommunikation kostenlos zu unterstützen.
- Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, wie Ärztinnen und Ärzte, Anwältinnen und Anwälte, Psychologinnen und Psycho-

logen, bedürfen besonders im Interesse ihrer Klientel eines umfassenden Schutzes ihrer Telekommunikation.

Straftaten gegen den Schutz der Privatsphäre ist wirksamer entgegenzutreten. Notwendig sind z. B. die Prüfung eines Verbots des freien Verkaufs von Abhörtechnik, eine Verbesserung der Strafverfolgung im Bereich illegaler Abhörmaßnahmen und eine Verschärfung des strafrechtlichen Schutzes des Fernmeldegeheimnisses.

6. Anlage: Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Risiken und Grenzen der Videoüberwachung

Immer häufiger werden Videokameras eingesetzt, die für Zwecke der Überwachung genutzt werden können. Ob auf Flughäfen, Bahnhöfen, in Ladenpassagen, Kaufhäusern oder Schalterhallen von Banken oder anderen der Öffentlichkeit zugänglichen Einrichtungen, überall müssen Bürgerinnen und Bürger damit rechnen, dass sie auf Schritt und Tritt offen oder heimlich von einer Videokamera aufgenommen werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht darin die Gefahr, dass diese Entwicklung zur einer Überwachungsinfrastruktur führt.

Mit der Videoüberwachung sind besondere Risiken für das Recht auf informationelle Selbstbestimmung verbunden. Weil eine Videokamera alle Personen erfasst, die in ihren Bereich kommen, werden von der Videoüberwachung unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen betroffen. Erfassung, Aufzeichnung und Übertragung von Bildern sind für die Einzelnen in aller Regel nicht durchschaubar. Schon gar nicht können sie die durch die fortschreitende Technik geschaffenen Bearbeitungs- und Verwendungsmöglichkeiten abschätzen und überblicken. Die daraus resultierende Ungewissheit, ob und von wem sie beobachtet werden und zu welchen Zwecken dies geschieht, erzeugt einen latenten Anpassungsdruck. Dies beeinträchtigt nicht nur die grundrechtlich garantierten individuellen Entfaltungsmöglichkeiten, sondern auch das gesellschaftliche Klima in unserem freiheitlichen und demokratischen Gemeinwesen insgesamt. Alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.

Daher müssen

- eine strenge Zweckbindung,
- eine differenzierte Abstufung zwischen Übersichtsaufnahmen, dem gezielten Beobachten einzelner Personen, dem Aufzeichnen von Bilddaten und dem Zuordnen dieser Daten zu bestimmten Personen,
- die deutliche Erkennbarkeit der Videoüberwachung für die betroffenen Personen,

- die Unterrichtung identifizierter Personen über die Verarbeitung ihrer Daten
- sowie die Löschung der Daten binnen kurzer Fristen

strikt sichergestellt werden.

Jede Einrichtung einer Videoüberwachung sollte der datenschutzrechtlichen Vorabkontrolle unterzogen werden. Das heimliche Beobachten und Aufzeichnen, die gezielte Überwachung bestimmter Personen sowie die Suche nach Personen mit bestimmten Verhaltensmustern müssen grundsätzlich verboten sein. Ausnahmen müssen im Strafprozessrecht und im Polizeirecht präzise geregelt werden. Videoüberwachung darf nicht großflächig oder flächendeckend installiert werden, selbst wenn jeder Einsatz für sich gesehen gerechtfertigt wäre. Auch ein zeitlich unbegrenzter Einsatz ohne regelmäßige Erforderlichkeitsprüfung ist abzulehnen. Der Schutz der Freiheitsrechte erfordert überdies, dass heimliches Aufzeichnen und unbefugte Weitergabe oder Verbreitung von Aufnahmen ebenso strafbewehrt sein müssen wie der Missbrauch videotechnisch gewonnener – insbesondere biometrischer – Daten und deren Abgleiche.

Dies bedeutet:

1. Bei einer gesetzlichen Regelung der Videoüberwachung durch öffentliche Stellen dürfen Einschränkungen nur aufgrund einer klaren Rechtsgrundlage erfolgen, die dem Grundsatz der Verhältnismäßigkeit Rechnung trägt.
 - Die Voraussetzungen einer Videoüberwachung und der mit ihr verfolgte Zweck müssen eindeutig bestimmt werden. *Dafür kommen – soweit nicht überwiegende schutzwürdige Belange von Betroffenen entgegenstehen – unter anderem in Betracht:* ¹⁾
 - die Beobachtung einzelner öffentlicher Straßen und Plätze oder anderer öffentlich zugänglicher Orte, auf denen wiederholt Straftaten begangen worden sind, solange tatsächliche Anhaltspunkte dafür bestehen, dass dort weitere Straftaten begangen werden (Kriminalitätsschwerpunkte) und mit der Beobachtung neben der Sicherung von Beweisen eine Präventionswirkung erreicht werden kann; der Grundsatz der Verhältnismäßigkeit ist dabei strikt zu beachten. Ungezielte Verlagerungsprozesse sollten vermieden werden.
 - für die Verkehrslenkung nur Übersichtsaufnahmen,

- der Schutz öffentlicher Einrichtungen im Rahmen der ordnungsbehördlichen Gefahrenabwehr, solange eine besondere Gefahrenlage besteht.
- Maßnahmen im Rahmen des Hausrechts dürfen den grundsätzlich unbeobachteten Besuch öffentlicher Gebäude nicht unverhältnismäßig einschränken.
- Die Videoüberwachung ist für die Betroffenen durch entsprechende Hinweise erkennbar zu machen.
- Bildaufzeichnungen sind nur zulässig, wenn und solange sie zum Erreichen des verfolgten Zweckes unverzichtbar sind. Die Anlässe, aus denen eine Bildaufzeichnung ausnahmsweise zulässig sein soll, sind im Einzelnen zu bezeichnen. Die Aufzeichnungen sind unverzüglich zu löschen, wenn sie hierzu nicht mehr erforderlich sind oder überwiegende schutzwürdige Belange von Betroffenen entgegenstehen.
- Werden die Aufnahmen einer bestimmten Person zugeordnet, ist diese zu benachrichtigen, sobald der Zweck der Speicherung dadurch nicht gefährdet wird.
- Zur Prüfung der Normeffizienz ist festzulegen, dass das jeweils zuständige Parlament jährlich über die angeordneten Maßnahmen, soweit sie mit einer Speicherung der erhobenen Daten verbunden sind, und die mit ihnen erreichten Ergebnisse unterrichtet wird.

Bei der Videoüberwachung muss in besonderer Weise den Grundsätzen der Datensparsamkeit und Datenvermeidung Rechnung getragen werden. Die Chancen, die die modernen Technologien für die Umsetzung dieser Grundsätze, insbesondere für die Reduzierung auf tatsächlich erforderliche Daten, bieten, sind zu nutzen.

2. Der Gesetzgeber ist auch aufgefordert, für die Videoüberwachung durch Private Regelungen zu schaffen, die den für die optisch-elektronische Beobachtung durch öffentliche Stellen geltenden Grundsätzen entsprechen. Dabei muss sichergestellt werden, dass optisch-elektronische Systeme, die die Identifizierung einzelner Personen ermöglichen, nur zur Abwehr von Gefahren für Personen und zum Schutz gewichtiger privater Rechte eingesetzt werden dürfen. Die privatrechtlichen Regelungen zum Schutz des eigenen Bildes durch das Vertragsrecht, das Deliktsrecht, das Besitz- und Eigentumsrecht, das Kunsturheberrecht und die dazu ergangene Rechtsprechung reichen nicht aus.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, dass die Gesetzgeber bei der Novellierung der Datenschutzgesetze und anderer Gesetze diese Grundsätze berücksichtigen.

¹⁾ Die kursiv gedruckte Passage wurde bei Stimmenthaltung der Datenschutzbeauftragten der Länder Brandenburg, Bremen, Mecklenburg-Vorpommern und Nordrhein-Westfalen angenommen.

7. Anlage: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 10. Oktober 2000

Auftragsdatenverarbeitung durch das Bundeskriminalamt

Im Rahmen der Neukonzeption des polizeilichen Informationssystems INPOL ist geplant, neben bundesweit verfügbaren Verbunddaten auch Landesdatenbestände im Wege der Auftragsdatenverarbeitung logisch getrennt in der INPOL-Datenbank zu speichern. Zudem sollen aufgrund bilateraler Absprachen landesspezifische Informationen in bestimmtem Umfang gespeichert werden können und ebenso gegenseitige Zugriffe einzelner Länder auf die Datenbestände ermöglicht werden.

§ 2 Abs. 5 des Bundeskriminalamtgesetzes lässt grundsätzlich eine Unterstützung der Länder bei deren Datenverarbeitung auf Ersuchen, also in Einzelfällen, zu. Diese Vorschrift kann auch herangezogen werden, wenn aufgrund besonderer Dringlichkeit, wie gegenwärtig bei der Realisierung von INPOL-neu, eine zeitlich befristete Auftragsdatenverarbeitung von Landesdaten geplant ist. Hierzu sind Ende vergangenen Jahres entsprechende Beschlüsse des Arbeitskreises II und der Innenministerkonferenz gefasst worden.

Diese Entwicklung birgt aus der Sicht der Datenschutzbeauftragten die Gefahr, dass weitere Beschlüsse folgen werden, die die dauerhafte Speicherung von Landesdaten beim BKA begründen; bereits jetzt sind Tendenzen deutlich, die zentralisierte Speicherung der Daten auch zur Erleichterung der gegenseitigen Zugriffe auf Landesdaten zu nutzen.

Die Notwendigkeit der zentralen Datenspeicherung beim Bundeskriminalamt wird im Wesentlichen mit Kosten- und Zeitargumenten begründet. Diese sind jedoch aus datenschutzrechtlicher Sicht nicht geeignet, eine Erweiterung der zentralen Datenverarbeitung beim Bundeskriminalamt zu begründen.

Die dauerhafte zentrale Datenhaltung beim BKA würde die informationelle Trennung von Landesdaten und Verbunddaten aufweichen; die in § 2 Abs. 1 BKA-Gesetz statuierte Schwelle, dass nur Daten über Straftaten von länderübergreifender, internationaler oder sonst erheblicher Bedeutung beim BKA verarbeitet werden dürfen, würde schleichend umgangen.

Eine dauerhafte zentrale Landesdatenhaltung beim Bundeskriminalamt beinhaltet eine neue, bei der augenblicklichen Rechtslage unakzeptable Qualität polizeilicher Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern dazu auf, die für die Datenverarbeitung beim Bundeskriminalamt gesetzlich gezogenen Grenzen strikt zu beachten. Sie appellieren an die Innenminister/-senatoren von Bund und Ländern, an den bisherigen Beschlüssen festzuhalten und die Polizeien der Länder, wie ursprünglich geplant, aufzufordern, unverzüglich eigene Datenverarbeitungsverfahren zu entwickeln. Bis zur Realisierung dieser Verfahren könnte allenfalls eine übergangsweise Lösung als Auftragsdatenverarbeitung unter Wahrung datenschutzrechtlicher Anforderungen ermöglicht werden. Daneben steht das Angebot des Bundeskriminalamtes, kostenlos Software von INPOL-neu zur Verfügung zu stellen. Diese Lösung würde auch das vorgetragene Kostenargument entkräften.

8. Anlage: Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000

Vom Bürgerbüro zum Internet – Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung

Bei der Modernisierung der öffentlichen Verwaltung soll insbesondere die Dienstleistungs- und Serviceorientierung verbessert werden. Dazu sollen unter anderem Dienstleistungen in multifunktionalen Servicecentern (Bürgeramt, Bürgerbüro, Bürgerladen, Kundencenter) gebündelt und die Möglichkeiten der modernen Informations- und Kommunikationstechnik intensiver genutzt werden (Information, Kommunikation und Transaktion über das Internet, Einrichtung von Call-Centern).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt alle Bemühungen, den Kontakt von Bürgerinnen und Bürgern mit den Verwaltungen schneller, einfacher, effektiver und insbesondere transparenter zu machen. Die Datenschutzbeauftragten erklären daher ihre ausdrückliche Bereitschaft, solche Entwicklungsprozesse konstruktiv zu begleiten.

Es ist aber unerlässlich, dass bei allen Lösungen eine sichere und vertrauliche Kommunikation zwischen Verwaltung und Bürgern sowie ein angemessener Schutz personenbezogener Daten gewährleistet wird. Nur Serviceangebote, die dem Recht auf informationelle Selbstbestimmung gerecht werden, nützen letztlich sowohl Bürgerinnen und Bürgern als auch der Verwaltung selbst.

Eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet deshalb Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung. Diese Empfehlungen sollen den Verwaltungen helfen, bei der Verbesserung ihrer Dienstleistungs- und Serviceorientierung den Forderungen nach Datenschutz und Datensicherheit gerecht zu werden. Diese Empfehlungen werden demnächst veröffentlicht und entsprechend der rechtlichen und technischen Entwicklung fortgeschrieben.

9. Anlage: Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000

Datensparsamkeit bei der Rundfunkfinanzierung

Die Finanzierung des öffentlich-rechtlichen Rundfunks ist derzeit Gegenstand öffentlicher Diskussion in der Politik und unter den Rundfunkanstalten selbst. Erörtert wird hierbei auch, ob die Erhebung von Rundfunkgebühren, die an das „Bereithalten eines Rundfunkempfangsgerätes“ anknüpfen, im Hinblick auf veränderte Gerätetechniken und bestehende Mängel im Verfahren modifiziert oder durch andere Finanzierungsformen ersetzt bzw. ergänzt werden sollte.

Künftig wird kaum noch überschaubar sein, welche Geräte zum Rundfunkempfang geeignet sind. Über die eigentlichen Fernseh- und Rundfunkgeräte hinaus ist dies bereits heute beispielsweise mit Personalcomputern, die über einen Internetzugang verfügen, oder mit bestimmten Mobiltelefonen möglich. In naher Zukunft werden neue Technologien wie UMTS weitere Empfangsmöglichkeiten eröffnen. Sofern der Besitz derartiger multifunktionaler Geräte zum Kriterium für die Rundfunkgebührenpflicht gemacht wird, würde das zu einer erheblichen Ausweitung von Datenabgleichen führen. Schon das gegenwärtig praktizierte Gebühreneinzugsverfahren erfordert in großem Umfang die Verarbeitung personenbezogener Daten. Nach den Angaben der Rundfunkanstalten meldet ein signifikanter Teil der Rundfunkteilnehmerinnen und -teilnehmer trotz der Verpflichtung hierzu seine Geräte nicht an. Um möglichst alle Gebührenpflichtigen zu erfassen, nutzen die Rundfunkanstalten Daten aus dem Melderegister, vom privaten Adresshandel und setzen vor Ort Rundfunkgebührenbeauftragte ein, die einzelne Haushalte aufsuchen. Damit wird in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung vieler gesetzestreuer Bürgerinnen und Bürger eingegriffen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesländer auf, einer Neuordnung ein Modell zu Grunde zu legen, das sich stärker als das bestehende System der Rundfunkfinanzierung an den Prinzipien der Datenvermeidung, Datensparsamkeit und Dezentralisierung orientiert. Nach ihrer Überzeugung lässt sich die verfassungsrechtlich gebotene Staatsferne und Funktionsfähigkeit des öffentlich-rechtlichen Rundfunks auch mit anderen, das Recht auf informationelle Selbstbestimmung weniger stark einschränkenden Finanzierungsmodellen als dem derzeit praktizierten gewährleisten.

10. Anlage: Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000

Datenschutzrechtliche Konsequenzen aus der Entschlüsselung des menschlichen Genoms

Bei der Entschlüsselung des menschlichen Genoms sind in den letzten Monaten wohl entscheidende Durchbrüche gelungen. Für mehr als 20, oft vererbliche Krankheiten sind bereits Gentests zu erwerben, mit denen in Labors analysiert werden kann, ob eine Erkrankung vorliegt bzw. in welchem Umfang ein Erkrankungsrisiko besteht. Viele dieser Krankheiten sind allerdings bisher nicht heil- oder behandelbar.

Gentechnische Untersuchungen beim Menschen eröffnen den Zugang zu höchstpersönlichen und hochsensiblen Informationen in einem Maße, das die Intensität bisheriger personenbezogener Informationen ganz erheblich übersteigt. Durch den genetischen Einblick in den Kernbereich der Privatsphäre, etwa in Gesundheitsdisposition, Anlagen der Persönlichkeitsstruktur oder den voraussichtlichen Lebensverlauf, entsteht eine ganz neue Qualität des Wissens und des Offenlegens von persönlichsten Daten. Sowohl für die Betroffenen als auch für dritte Personen, insbesondere Familienangehörige, ist es von entscheidender Bedeutung, ob und inwieweit sie selbst und wer außer ihnen von den Ergebnissen Kenntnis bekommt. Davor steht die Frage, ob und aus welchen Anlässen überhaupt genetische Untersuchungen am Menschen vorgenommen werden dürfen. Zur informationellen Selbstbestimmung gehört auch das Recht auf Nichtwissen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass für die Zulässigkeit gentechnischer Untersuchungen beim Menschen und für den Umgang mit den dabei gewonnenen Informationen sehr schnell klare und verbindliche Prinzipien entwickelt werden, um auch die informationelle Selbstbestimmung in diesem Kernbereich zu sichern und zugleich eine „genetische Diskriminierung“ bei der Gewinnung oder Verwendung genetischer Informationen, etwa im Arbeitsverhältnis oder beim Abschluss von Versicherungsverträgen, zu verhindern. Auf der Grundlage dieser und in der „Entschließung über Genomanalyse und informationelle Selbstbestimmung“ vom 26. Oktober 1989 formulierten Grundsätze wird die Konferenz an der Ausgestaltung mitwirken.

Die Datenschutzbeauftragten erinnern an ihre Grundsätze aus der Entschließung von 1989 bezüglich der Genomanalyse:

- Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.
- Die jederzeit widerrufliche Einwilligung muss sich auch auf die weitere Verwendung der gentechnischen Informationen erstrecken. Im Falle eines Widerrufs sind die gewonnenen Informationen zu löschen oder an den Betroffenen herauszugeben.
- Jede Genomanalyse muss zweckorientiert vorgenommen werden. Es ist diejenige genomanalytische Methode zu wählen, die keine oder die geringste Menge an Überschussinformationen bringt. Überschussinformationen sind unverzüglich zu vernichten.
- Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.
- Die Genomanalyse im gerichtlichen Verfahren muss auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genomanalytischen Methoden angewandt werden, die Überschussinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u. a. sicherstellen, dass genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.
- Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.
- Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschießen, unvereinbar. Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.
- Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwerwiegenden Gesundheitsschädigung des Kindes führen würden, dass ein Schwangerschaftsabbruch straffrei bliebe.

Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können.

Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck, muss vermieden werden.

Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muss berücksichtigt werden. Demnächst werden nicht nur – wie bisher – Gensequenzen aufgedeckt und verglichen, sondern auch die mit dem Genom verbundenen Wirkungszusammenhänge für die menschliche Gesundheit und für die Persönlichkeitsstruktur entschlüsselt werden können.

11. Anlage: Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000

Entschließung zur Novellierung des BDSG

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an Bundestag und Bundesrat, das Gesetzgebungsverfahren eines novellierten Bundesdatenschutzgesetzes zügig und ohne Abstriche zum Abschluss zu bringen. Damit wird die längst überfällige Anpassung des deutschen Datenschutzrechts an die Vorgaben der EG-Richtlinie vorgenommen. Die Novelle enthält verschiedene innovative Ansätze, insbesondere das Gebot zur Datenvermeidung und Datensparsamkeit bei der Systemgestaltung (Systemdatenschutz – § 3a E-BDSG) und die Einführung des Datenschutzaudit (§ 9a), die von den Datenschutzbeauftragten schon seit langem befürwortet werden.

Sowohl der Systemdatenschutz als auch das Datenschutzaudit werden die Durchsetzung datenschutzfreundlicher Lösungen im Wettbewerb erleichtern und tragen auf diese Weise zur Selbstregulierung des Marktes bei. Das Datenschutzaudit fügt sich in die bewährten Strukturen des betrieblichen Datenschutzes ein und ermöglicht es den Unternehmen, datenschutzkonforme Angebote und Verhaltensweisen nachprüfbar zu dokumentieren und damit einen Wettbewerbsvorsprung zu gewinnen.

Die Konferenz fordert den Bundesrat auf, die Aufnahme des Datenschutzaudit in das BDSG nicht zu blockieren. Sie geht weiter davon aus, dass die angekündigte zweite Stufe der Novellierung des BDSG noch in dieser Legislaturperiode realisiert wird, und erklärt ihre Bereitschaft, hieran konstruktiv mitzuwirken.

12. Anlage: Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001

Datenschutz beim elektronischen Geschäftsverkehr

Die Konferenz wendet sich mit Entschiedenheit gegen Anträge, die gegenwärtig dem Bundesrat zum Entwurf eines Gesetzes zum elektronischen Geschäftsverkehr (BR-Drs. 136/01) vorliegen. Danach sollen Bestands- und Nutzungsdaten bei Telediensten nicht nur an Strafverfolgungsbehörden, sondern auch an Verwaltungsbehörden zur Verfolgung von Ordnungswidrigkeiten und an Nachrichtendienste übermittelt werden. Darüber hinaus sollen die Anbieterinnen und Anbieter zur Speicherung von Nutzungsdaten auf Vorrat für eine mögliche spätere Strafverfolgung verpflichtet werden.

Die Datenschutzbeauftragten weisen darauf hin, dass sich anhand dieser Daten nachvollziehen lässt, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen nachgeht. Eine pauschale Registrierung jeder Inanspruchnahme von Telediensten zur staatlichen Überwachung greift tief in das Persönlichkeitsrecht der betroffenen Nutzerinnen und Nutzer ein und berührt auf empfindliche Weise deren Informationsfreiheit. Der Bundesrat wird daher aufgefordert, diese Anträge abzulehnen.

13. Anlage: Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001

Novellierung des G 10-Gesetzes

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 Schwere der Kriminalität 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 wei-

ter 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 nicht-leitungsgebundenen, 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 "strategischer Überwachung" nach § 5 G 10-E. Dies setzt eine hohe Eingriffsschwelle und enge zeitliche Befristungen voraus, die der Entwurf nicht hinreichend vorsieht.

14. Anlage: Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001

Datenschutz bei der Bekämpfung von Datennetzkriminalität

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

15. Anlage: Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001

Äußerungsrecht der Datenschutzbeauftragten

Die Datenschutzbeauftragten des Bundes und der Länder sind verpflichtet, Einzelne – wie es die Rechtsprechung des Bundesverfassungsgerichts und die Richtlinie der Europäischen Gemeinschaft zum Datenschutz von 1995 vorsehen – vor rechtswidrigem Umgang mit ihren personenbezogenen Daten wirksam zu schützen. Die damit verbundenen Beratungs- und Kontrollaufgaben verleihen den Datenschutzbeauftragten ein öffentliches Wächteramt, das die Befugnis einschließt, Behördenverhalten auch im Detail und, soweit der Bedeutung der Sache angemessen, auch unter Bezeichnung der Amtsträgerinnen und Amtsträger öffentlich zu rügen.

Aus gegebenem Anlass wendet sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder energisch gegen Versuche im Land Sachsen, durch gesetzgeberische Maßnahmen dieses Recht zu beschneiden und die Arbeit des Sächsischen Datenschutzbeauftragten zu behindern.

16. Anlage: Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001

Informationszugangsgesetze

Die Konferenz verfolgt mit Interesse die Bestrebungen des Bundes, ein Informationszugangsgesetz zu schaffen und dem Bundesbeauftragten für den Datenschutz die Aufgaben zur Sicherung des Informationszugangs zu übertragen. Die Bundesregierung nimmt damit die Überlegungen auf, die in Artikel 255 EU-Vertrag und Artikel 42 EU-Grundrechte-Charta zum Ausdruck kommen. Die Konferenz betont, dass das Recht auf informationelle Selbstbestimmung der Einzelnen dem freien Zugang zu behördeninternen, amtlichen Informationen nicht entgegen steht, wenn die Privatsphäre der Betroffenen sowie Betriebsgeheimnisse gesetzlich geschützt bleiben. Die Berichte aus den Ländern Berlin, Brandenburg und Schleswig-Holstein zeigen, dass die datenschutzrechtlichen Gewährleistungen für die informationelle Selbstbestimmung sich mit dem erweiterten Zugangsrecht zu den Informationen öffentlicher Stellen unter der Voraussetzung entsprechender Schutzmechanismen vereinbaren lassen. Die Zusammenführung von Datenschutz- und Informationszugangskontrolle kann diese Gewährleistung institutionell absichern.

17. Anlage: Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001

Novellierung des Melderechtsrahmengesetzes

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 Internet-gestützten Abruf die gesetzlich vorgeschriebene Berücksichtigung der schutzwürdigen Belange Betroffener nicht möglich ist, sollte für die Bürgerin oder den Bürger in diesen Fällen ein ausdrückliches Einwilligungsgesetz 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 Daten-

schutzbeauftragten 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.

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

Veröffentlichung von Insolvenzinformationen im Internet

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 Auskunftsteile 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, aufgrund 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. Bevor die geplante Änderung des § 9 InsO verabschiedet wird, ist daher vorrangig zu klären, wie das Recht auf informationelle Selbstbestimmung der Betroffenen besser geschützt werden kann.

Auch in anderen Bereichen wird das Internet bereits genutzt, erprobt oder die Nutzung erwogen, um justizielle Informationen bereitzustellen, z. B. die Handels-, Vereins-, Genossenschafts- und Partnerschaftsregister oder in Zwangsvollstreckungsverfahren. Inwieweit das Internet als Medium der im Ergebnis unbegrenzten Informationsverarbeitung datenschutzrechtlich angemessen ist und welches Datenprofil ins Internet eingestellt werden darf, muss differenziert in Übereinstimmung mit dem gesetzlich bezweckten Grad der Publizität der jeweiligen Daten entschieden werden. Jede gesetzgeberische Entscheidung für eine Veröffentlichung über das Internet sollte aber im Hinblick auf deren besondere Risiken regeln, dass Veröffentlichungen befristet sind und dass spezielle Vorkehrungen getroffen werden, um die Identität und die Authentizität zu sichern sowie eine automatische Übernahme der Daten zu verhindern (Kopierschutz).

Sollte sich der Gesetzgeber nach sorgfältiger Abwägung für eine Veröffentlichung über das Internet entscheiden, so muss er die Auswirkungen der Regelung auf Grund aussagefähiger Berichte der Landesjustizverwaltungen überprüfen. Gegenstand dieser Überprüfung muss auch sein, ob die eingetretene Kostensenkung tatsächlich, wie von der Bundesregierung erwartet, einer größeren Anzahl von Schuldnerinnen und Schuldnern den Weg zur Restschuldbefreiung eröffnet hat.

19. Anlage: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 10. Mai 2001

zum Entwurf der Telekommunikations-Überwachungsverordnung

Das Bundesministerium für Wirtschaft hat Ende Januar 2001 den Entwurf für eine Telekommunikations-Überwachungsverordnung (TKÜV) vorgelegt, der in Kürze dem Bundeskabinett zugeleitet wird. Der Entwurf basiert auf dem Telekommunikationsgesetz, das den Begriff der Telekommunikation weit fasst. Da er technikneutral formuliert ist, werden von den Überwachungsmaßnahmen nicht nur die Sprachtelefonie und der Telefaxverkehr, sondern auch alle anderen elektronischen Kommunikationsplattformen und damit insbesondere auch das Internet erfasst.

Sobald ein Internet-Provider einen E-Mail-Dienst anbietet, muss er technische Einrichtungen zur Umsetzung der Überwachungsmaßnahmen vorhalten, obwohl die Vermittlung des Zugangs zum Internet als anmelde- und zulassungsfreier Teledienst nicht zu den Telekommunikationsdiensten gehört. Diese Verpflichtung der Internet-Provider macht es technisch möglich, künftig den gesamten Internet-Verkehr, also auch das bloße "Surfen" zu überwachen. Dies ist aber nach deutschem Recht so nicht vorgesehen. Bedenklich ist in diesem Zusammenhang, dass das European Telecommunications Standards Institute (ETSI) gegenwärtig an einem technischen Standard arbeitet, der den Lauschangriff auf IP-Netze (Internet) und die Überwachung des gesamten Internet-Verkehrs europaweit vereinheitlichen soll.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden dagegen, eine technische Infrastruktur zu schaffen, die jederzeit eine umfassende Überwachung des Internet-Verkehrs möglich macht. Eine derartige Überwachung würde einen unverhältnismäßigen Eingriff in das Grundrecht auf Persönlichkeitsschutz darstellen und darüber hinaus den im Teledienstedatenschutzgesetz und im Mediendienstestaatsvertrag normierten Grundsätzen der Datenvermeidung und der Datensparsamkeit zuwiderlaufen.

Es muss sichergestellt werden, dass die zunehmende Nutzung von Telediensten zu Alltagsgeschäften auch künftig generell überwachungsfrei bleibt. Die bestehenden materiellen Befugnisse zur Telekommunikationsüberwachung im Strafprozessrecht, G 10-Gesetz und im Außenwirtschaftsgesetz bedürfen zudem insgesamt dringend einer kritischen Evaluation und Bereinigung, die die Bundesregierung durch eine wissenschaftliche Untersuchung der Effektivität bisheriger Überwachungsanordnungen bereits eingeleitet hat.

Die Datenschutzbeauftragten des Bundes und der Länder fordern ebenso eine Evaluation der Telekommunikations-Überwachungsverordnung, die im Lichte der Ergebnisse der Untersuchung über die Effektivität von Telekommunikations-Überwachungsmaßnahmen vorzunehmen ist.

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

Sondertreffen der Datenschutzbeauftragten des Bundes und der Länder zur Terrorismusbekämpfung

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.

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

Freiheits- und Persönlichkeitsrechte dürfen bei der Terrorismusbekämpfung nicht verloren gehen

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 unververtretbare 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.

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

EUROJUST – Vorläufer einer künftigen europäischen Staatsanwaltschaft?

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 Rechts-hilfeersuchen 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 die-

ser 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.

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

Datenschutzrechtliche Anforderungen an den “Arzneimittelpass” (Medikamentenchipkarte)

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 offen legen, 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.

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

Lkw-Maut auf Autobahnen und allgemeine Maut auf privat errichteten Bundesfernstraßen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, bei der technischen Realisierung und bei der anstehenden internationalen Normierung elektronischer Mautsysteme datenschutzrechtliche Anforderungen durchzusetzen.

Das Bundeskabinett hat am 15. August 2001 den Gesetzentwurf für die Einführung eines solchen Mautsystems beschlossen. Ab 2003 ist neben der manuellen Erfassung der Gebühren ein automatisches System geplant, mit dem eine streckenbezogene Autobahnbenutzungsgebühr (Maut) für Lastkraftwagen erhoben werden soll. Das Bundesministerium für Verkehr, Bau- und Wohnungswesen prüft zurzeit Angebote, die im Ergebnis einer europaweiten Ausschreibung eingegangen sind.

Für das automatische System sollen das Satellitennavigationssystem GPS und die Mobilfunktechnologie genutzt werden. Dadurch werden stationäre Erfassungseinrichtungen entbehrlich. Relativ einfach könnte so das mautpflichtige Straßennetz beispielsweise auf den Bereich der Bundesstraßen ausgedehnt werden. Selbst ein grenzüberschreitender Einsatz derartiger Systeme wäre aus technischer Sicht leicht zu realisieren. Entsprechendes Interesse aus dem benachbarten Ausland ist bereits bekundet worden.

Die verfügbare, im Gesetzentwurf nicht festgeschriebene Technik ermöglicht es prinzipiell, den Fahrweg der Mautpflichtigen detailliert zu dokumentieren und zu archivieren und auf diese Weise exakte Bewegungsprofile zu erstellen. Damit würden die Voraussetzungen geschaffen, dass Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Die Datenschutzbeauftragten des Bundes und der Länder halten es deshalb für unverzichtbar, elektronische Mautsysteme datenschutzgerecht auszugestalten. Insbesondere ist dafür Sorge zu tragen, dass die Erhebung und Speicherung ausschließlich für Abrechnungszwecke verwendet werden.

Weiterhin ist bei Gestaltung und beim Betrieb der erforderlichen Erfassungs- und Kontrollsysteme das im Bundesdatenschutzgesetz normierte Prinzip der Datensparsamkeit sicherzustellen. Das erfordert den Einsatz von Verfahren, bei denen Mautgebühren vorab entrichtet werden können, ohne dass dafür die Erhebung und Speicherung personenbezogener Daten erforderlich ist.

Insbesondere ist sicherzustellen, dass damit keine oder so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden. Soweit personenbezogene Daten beispielsweise für Abrechnungs- oder Kontrollzwecke gespeichert werden, sind sie zum frühestmöglichen Zeitpunkt, spätestens jedoch nach Entrichtung der Straßenbenutzungsgebühr beziehungsweise nach Abschluss eines Mauterstattungsverfahrens zu löschen, wenn sie nicht mehr für die Abwicklung des Mautverfahrens oder für erforderliche Kontroll- oder Prüfverfahren benötigt werden.

Bereits 1995 haben die Datenschutzbeauftragten des Bundes und der Länder Anforderungen an Systeme zur automatischen Erhebung von Straßennutzungsgebühren formuliert. Insbesondere die folgenden Aspekte sind nach wie vor aktuell:

- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Identität der Mautpflichtigen darf nur dann aufgedeckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Gebühren nicht entrichtet worden sind.
- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Mautpflichtigen durchschaubar sein. Sie müssen sich jederzeit über den Abrechnungsvorgang informieren sowie den eventuellen Kontrollvorgang erkennen können.
- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, dass sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.
- Es ist sicherzustellen, dass anfallende personenbezogene Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen.

Außerdem liegt ein Gesetzentwurf vor, der zur Erhebung von Mautgebühren an Brücken, Tunneln und Gebirgspässen im Zuge von Bundesautobahnen und Bundesstraßen sowie an mehrspurigen Bundesstraßen mit getrennten Fahrbahnen berechtigt, soweit sie von Privaten errichtet sind. Die Mautpflicht gilt für alle Kraftfahrzeuge. Deshalb muss an der im Entwurf vorgesehenen Barzahlungsmöglichkeit ohne Verarbeitung personenbezogener Daten unbedingt festgehalten werden. Ihre Ausgestaltung sollte kundenfreundlich erfolgen. Diese Zahlungsweise vermeidet die weitergehende Datenerfassung für alle Mautpflichtigen (Kennzeichen und Bilder der Fahrzeuge). In der zu erlassenden Rechtsverordnung muss deshalb insbesondere sichergestellt werden, dass keine Datenerfassung bei Personen erfolgt, die die Gebühr unmittelbar entrichten.

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

Neue Medienordnung

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.

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

Biometrische Merkmale in Personalausweisen und Pässen

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.

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

Gesetzliche Regelung von genetischen Untersuchungen

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 entgegenzunehmen;

- 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 zur Entschließung

Vorschläge zur Sicherung der Selbstbestimmung bei genetischen Untersuchungen

Allgemeines

Gegenstand

Zu regeln ist die Zulässigkeit genetischer Untersuchungen beim Menschen, der Umgang mit Proben und die Erhebung, Verarbeitung und Nutzung genetischer Daten. Neben allgemeinen Regelungen sind besondere Bestimmungen zu genetischen Untersuchungen

1. zu medizinischen Zwecken
2. im Zusammenhang mit Arbeits- und Versicherungsverhältnissen
3. zur Abstammungsklä rung und Identifizierung außerhalb der Strafverfolgung
4. zu Forschungszwecken

zu treffen.

Ziel, Benachteiligungsverbot

(1) Ziel der Regelungen ist der Schutz der Menschenwürde, der Persönlichkeit und der informationellen Selbstbestimmung der Betroffenen bei genetischen Untersuchungen.

(2) Niemand darf wegen seiner Erbanlagen oder wegen der Weigerung, eine genetische Untersuchung bei sich durchführen zu lassen, benachteiligt werden.

Begriffe

1. *Genetische Untersuchungen*: Untersuchungen auf Chromosomen-, Genprodukt- oder molekularer DNS / RNS-Ebene, die darauf abzielen, Informationen über das Erbgut zu erhalten;
2. *Prädiktive Untersuchungen*: vor- oder nachgeburtliche genetische Untersuchungen mit dem Ziel, Erbanlagen einer Person, insbesondere Krankheitsanlagen vor dem Auftreten von Symptomen oder einen Überträgerstatus, zu erkennen;
3. *Überträgerstatus*: Erbablagen, die erst in Verbindung mit entsprechenden Erbanlagen eines Partners oder einer Partnerin eine Krankheitsanlage bei den gemeinsamen Nachkommen ausbilden;
4. *Pränatale Untersuchungen*: vorgeburtliche genetische Untersuchungen mit dem Ziel, während der Schwangerschaft Informationen über das Erbgut des Embryos oder des Fötus zu gewinnen;
5. *Reihenuntersuchung*: genetische Untersuchungen, die systematisch der gesamten Bevölkerung oder bestimmten Gruppen der Bevölkerung angeboten werden, ohne dass bei den Betroffenen Anhaltspunkte dafür bestehen, dass die gesuchten Erbanlagen bei ihnen vorhanden sind;
6. *Diagnostische genetische Untersuchungen*: genetische Untersuchungen zur Abklärung der Diagnose einer manifesten Erkrankung oder zur Vorbereitung oder Verlaufskontrolle einer Behandlung;
7. *Probe*: die für eine genetische Untersuchung vorgesehene oder genutzte biologische Substanz;
8. *Genetische Daten*: im Zusammenhang mit genetischen Untersuchungen erlangte Informationen über eine Person;
9. *Betroffene Person*: die Person, von der eine Probe vorliegt oder deren genetische Daten erhoben, verarbeitet oder genutzt werden; bei pränatalen Untersuchungen auch die schwangere Frau;
10. *Verarbeiten*: das Speichern, Verändern, Übermitteln, Sperren und Löschen erhobener personenbezogener genetischer Daten.

Zulässigkeit genetischer Untersuchungen

Genetische Untersuchungen, der Umgang mit Proben und die Erhebung, Verarbeitung und Nutzung genetischer Daten bedürfen der freiwilligen, schriftlichen Einwilligung der betroffenen Person nach Aufklärung. Vorbehalten bleiben die in einem Gesetz über genetische Untersuchungen zu regelnden und in der Strafprozessordnung geregelten Ausnahmen.

Zulassung zur Durchführung genetischer Untersuchungen

- (1) Wer genetische Untersuchungen durchführen will, bedarf hierfür der Zulassung durch die zuständige Aufsichtsbehörde des Landes.
- (2) Die Zulassung wird erteilt, wenn Gewähr dafür besteht, dass
 - die Untersuchungen und ihre Auswertungen sorgfältig und nach dem Stand von Wissenschaft und Technik durchgeführt werden,
 - die Regelungen gemäß diesen Vorschlägen eingehalten, insbesondere Information und Beratung der betroffenen Person und die Datensicherheit gewährleistet werden und
 - in der antragstellenden Person die berufsrechtlichen und gewerberechtlichen Voraussetzungen vorliegen.
- (3) Das Nähere regelt die Bundesregierung durch Rechtsverordnung.

Inverkehrbringen genetischer Tests und Angebote von genetischen Untersuchungen

Genetische Testverfahren dürfen nur für den Gebrauch durch Ärztinnen, Ärzte oder Labors eingeführt oder in Verkehr gebracht werden. Das öffentliche Angebot, genetische Untersuchungen zu medizinischen Zwecken ohne individuelle Beratung der betroffenen Person durchzuführen, ist unzulässig. Die Berufsfreiheit, Artikel 12 Absatz 1 Satz 2 Grundgesetz, wird insoweit eingeschränkt.

Zweckbindung

Die für die genetische Untersuchung vorgesehene oder genutzte Probe und die genetischen Daten dürfen nur für den Zweck verwandt und für die Dauer aufbewahrt werden, zu denen die betroffene Person ihre Einwilligung erklärt hat oder zu denen ein Gericht oder eine Verwaltungsbehörde eine Anordnung getroffen hat. Vorbehalten bleiben die in einem Gesetz über genetische Untersuchungen geregelten Ausnahmen.

Datensicherheit

- (1) Proben und genetische Daten sind vor dem Zugriff unbefugter Dritter wirksam zu schützen. Dies gilt auch in Bezug auf Mitarbeiterinnen und Mitarbeiter der untersuchenden und datenverarbeitenden Stelle, die an der genetischen Untersuchung, Aufklärung und Beratung nicht beteiligt sind oder waren.
- (2) Genetische Daten sind von anderen Datenarten gesondert zu speichern.
- (3) Im Übrigen gilt hinsichtlich der genetischen Daten die Bestimmung des Bundesdatenschutzgesetzes über die technischen und organisatorischen Maßnahmen der Datensicherheit in der jeweils geltenden Fassung.

Einsichts- und Auskunftsrecht

Die betroffene Person hat das Recht, unentgeltlich Einsicht in die Dokumentationen zur genetischen Untersuchung einschließlich Aufklärung und Beratung zu nehmen und Auskunft über die zu ihr gespeicherten Daten zu verlangen.

Genetische Untersuchungen zu medizinischen Zwecken

Grundsatz

- (1) Zu medizinischen Zwecken dürfen prädiktive Untersuchungen nur durchgeführt werden, wenn sie nach ärztlicher Indikation der Vorsorge, der Behandlung oder der Familienplanung der betroffenen Person dienen.
- (2) Eine genetische Untersuchung zum Erkennen eines Überträgerstatus ist nur zu Zwecken der konkreten Familienplanung zulässig.
- (3) Für diagnostische genetische Untersuchungen gelten nur die Anforderungen gemäß dem Arztvorbehalt (siehe unten) und an diagnostische genetische Untersuchungen bei behinderten Personen (siehe am Ende dieses Abschnitts).

Pränatale Untersuchungen

Pränatale Untersuchungen sind auf das Erkennen solcher Krankheiten zu richten, die vorgeburtlich behandelt werden können. Für darüber hinausgehende genetische Untersuchungen gelten die Richtlinien der Bundesärztekammer zur pränatalen Diagnostik. Das Geschlecht darf gezielt nur zu medizinischen Zwecken festgestellt werden.

Ob darüber hinaus auch schwere Behinderungen und Anlagen für schwere, nicht behandelbare Krankheiten Ziele pränataler DNA-Untersuchungen sein dürfen, muss der gesellschaftspolitischen Diskussion, der fachmedizinischen Bewertung und der Verantwortung des Gesetzgebers überlassen bleiben.

Genetische Untersuchungen bei Minderjährigen und nicht einsichtsfähigen Erwachsenen

- (1) Genetische Untersuchungen bei Minderjährigen sind nur zulässig, wenn ihre Durchführung vor Erreichen der Volljährigkeit erforderlich ist, um den Ausbruch einer Krankheit zu vermeiden oder zu verzögern, eine Heilung oder Verlaufsmilderung zu erreichen oder spätere besonders belastende Untersuchungen zu vermeiden. Bei Aufklärung, Beratung und Einwilligung (siehe unten) ist die Einsichtsfähigkeit der betroffenen minderjährigen Person zu berücksichtigen.
- (2) Prädiktive Untersuchungen bei nicht einsichtsfähigen Erwachsenen dürfen sich nur auf das Erkennen von Krankheiten richten, deren Ausbruch vermieden oder verzögert oder bei denen eine Heilung oder Verlaufsmilderung erreicht werden kann. Die Einwilligung obliegt dem gesetzlichen Vertreter.

Reihenuntersuchungen

- (1) Genetische Reihenuntersuchungen bedürfen der Zulassung durch die zuständige Landesbehörde.
- (2) Voraussetzung für die Zulassung ist, dass
 - die Reihenuntersuchung gerichtet ist auf das Erkennen von verbreiteten oder schweren Krankheiten, die unverzüglich nach dem Untersuchungsergebnis behandelt werden können, oder von Krankheiten, deren Ausbruch verhindert werden kann,

- die Untersuchungsmethode eindeutige Ergebnisse liefert,
- die Freiwilligkeit der Teilnahme und die genetische Beratung gewährleistet und
- der Datenschutz gesichert ist.

Arztvorbehalt

- (1) Prädiktive Untersuchungen dürfen nur von Fachärztinnen und Fachärzten für Humangenetik veranlasst werden. Diagnostische genetische Untersuchungen dürfen auch von anderen zur Berufsausübung zugelassenen Ärztinnen und Ärzten veranlasst werden.
- (2) Die veranlassende Ärztin oder der veranlassende Arzt hat die Aufklärung und Beratung (siehe nachstehend) und die Einholung und Dokumentation der Einwilligung (siehe unten) sicherzustellen.

Aufklärung und Beratung

- (1) Vor und nach einer prädiktiven genetischen Untersuchung ist die betroffene Person umfassend aufzuklären und zu beraten, um ihr eine selbstbestimmte Entscheidung gemäß den Anforderungen an die Einwilligung (siehe unten) zu ermöglichen.
- (2) Die betroffene Person und gegebenenfalls ihr gesetzlicher Vertreter muss insbesondere aufgeklärt werden über
 - Ziel, Art, Aussagekraft und Risiko der Untersuchung und die Folgen ihrer Unterlassung,
 - mögliche, auch unerwartete Ergebnisse der Untersuchung,
 - mögliche Folgen des Untersuchungsergebnisses, einschließlich physischer und psychischer Belastungen der betroffenen Person oder ihrer Familie,
 - Behandlungsmöglichkeiten für die gesuchte Krankheit,
 - den geplanten Umgang mit der Probe und den genetischen Daten einschließlich des Orts und der Dauer der Aufbewahrung bzw. Speicherung,

- die Einflussmöglichkeiten und Datenschutzrechte der betroffenen Person,
 - weitere Beratungs- und Unterstützungsmöglichkeiten.
- (3) Aufklärung und Beratung dürfen nur der individuellen und familiären Situation der betroffenen Person und den möglichen psychosozialen Auswirkungen des Untersuchungsergebnisses auf sie und ihre Familie Rechnung tragen.
 - (4) Bei Reihenuntersuchungen kann in begründeten Ausnahmefällen die Aufklärung in standardisierter Form erfolgen, wenn zugleich die Möglichkeit einer zusätzlichen individuellen Beratung angeboten wird.
 - (5) Bei pränatalen Untersuchungen ist der Partner der betroffenen Frau in die Beratung einzubeziehen, sofern die Frau einwilligt. Auf Stellen der Schwangerschaftskonfliktberatung ist hinzuweisen.
 - (6) Bei genetischen Untersuchungen zum Erkennen eines Überträgerstatus soll der Partner oder die Partnerin der betroffenen Person in die Aufklärung und Beratung einbezogen werden.

Einwilligung

- (1) Nach der Aufklärung und Beratung entscheidet die betroffene Person nach angemessener Bedenkzeit in freier Selbstbestimmung darüber,
 - ob die genetische Untersuchung durchgeführt werden soll,
 - welches Ziel die genetische Untersuchung hat,
 - ob sie auch unvermeidbare weitere Untersuchungsergebnisse zur Kenntnis nehmen will,
 - wie gegebenenfalls mit der Probe und den genetischen Daten weiter verfahren werden soll.

Soweit die betroffene Person vom Ergebnis, auf das die Untersuchung zielt, keine Kenntnis nehmen will, soll außer bei Reihenuntersuchungen grundsätzlich auf die genetische Untersuchung verzichtet werden.

- (2) Die betroffene Person oder ihr gesetzlicher Vertreter hat die vorherige Aufklärung und Beratung schriftlich zu bestätigen und die Einwilligung in die genetische Untersuchung und in den vereinbarten Umgang mit der Probe und den genetischen Daten schriftlich zu erklären.
- (3) Die Einwilligung kann widerrufen werden mit der Folge, dass noch nicht erfolgte Maßnahmen unterbleiben, schon vorliegende Proben vernichtet und die im Zusammenhang mit der Untersuchung erhobenen und gespeicherten Daten gelöscht werden.

Unterrichtung über das Untersuchungsergebnis

- (1) Die veranlassende Ärztin oder der veranlassende Arzt teilt das Ergebnis der genetischen Untersuchung nur der betroffenen Person, bei Minderjährigen auch oder nur ihrem gesetzlichen Vertreter mit und berät über die möglichen Folgen und Entscheidungsalternativen.
- (2) Ist das Ergebnis nach ärztlicher Erkenntnis auch für Verwandte der betroffenen Person von Bedeutung, hat die Ärztin oder der Arzt bei der nachgehenden Beratung der betroffenen Person auch auf das Recht der Verwandten hinzuweisen, ihre Erbanlagen nicht zur Kenntnis zu nehmen. Will die betroffene Person die Verwandten gleichwohl unterrichten, soll die Beratung auch die Möglichkeit umfassen, die Ärztin oder den Arzt mit der Unterrichtung von Verwandten der betroffenen Person zu beauftragen.
- (3) Gegen den Willen der betroffenen Person oder ihres gesetzlichen Vertreters darf die veranlassende Ärztin oder der veranlassende Arzt Verwandte oder Partner der betroffenen Person nur dann von dem Untersuchungsergebnis unterrichten, wenn und soweit dies zur Wahrung erheblich überwiegender Interessen dieser Personen erforderlich ist.

Diagnostische genetische Untersuchung bei behinderten Personen

Bei diagnostischen genetischen Untersuchungen, die sich auf die Ursache einer Behinderung der betreffenden Person beziehen, gelten die Anforderungen an die Einwilligung und Unterrichtung über das Untersuchungsergebnis entsprechend.

Genetische Untersuchungen im Zusammenhang mit Arbeits- und Versicherungsverhältnissen

Grundsatz

Arbeitgebern und Versicherern ist es verboten, als Voraussetzung für einen Vertragsabschluss oder während des Vertragsverhältnisses prädiktive genetische Untersuchungen an betroffenen Arbeits- oder Versicherungsvertragsbewerbern oder Vertragspartnern durchzuführen oder zu veranlassen oder Ergebnisse von genetischen Untersuchungen zu verlangen, entgegenzunehmen oder sonst zu nutzen. Aus einer wahrheitswidrigen Beantwortung können Arbeitgeber oder Versicherer grundsätzlich keine Rechte ableiten (Ausnahmen siehe unten).

Arbeitsverhältnis

Bleibt der Arbeitsplatz trotz vorrangiger Arbeitsschutzmaßnahmen mit einer erhöhten Erkrankungs- oder Unfallgefahr verbunden, für deren Eintritt nach dem Stand der Wissenschaft eine bestimmte Genstruktur der Betroffenen von Bedeutung ist, ist eine Arbeitsplatzbewerberin oder ein Arbeitsplatzbewerber hierauf hinzuweisen. Die Betriebsärztin oder der Betriebsarzt soll die betroffene Person hinsichtlich einer geeigneten genetischen Untersuchung beraten und ihr dafür zugelassene Ärztinnen oder Ärzte benennen.

Ausnahmen für das Versicherungsverhältnis

- (1) Strebt die betroffene Person eine Versicherung mit einer Leistungssumme über 250.000 € an, ist der Versicherer berechtigt zu fragen, ob und gegebenenfalls wann bei der betroffenen Person eine prädiktive genetische Untersuchung durchgeführt wurde. Bei arglistigem Verschweigen kann der Versicherer den Versicherungsvertrag kündigen.
- (2) Bestehen konkrete Anhaltspunkte, insbesondere aufgrund des Zeitabstandes zwischen genetischer Untersuchung und Versicherungsantrag, dafür, dass die Höhe der gewünschten Versicherungsleistung mit dem Ergebnis der genetischen Untersuchung zusammenhängt, kann der Versicherer das Ergebnis der genetischen Untersuchung verlangen. Dies gilt nicht für eine genetische Untersuchung, die bei der betroffenen Person pränatal oder während der Minderjährigkeit oder

einer Einsichtsunfähigkeit durchgeführt wurde. In diesen Fällen darf der Versicherer das Ergebnis der genetischen Untersuchung von der betroffenen Person entgegennehmen.

Genetische Untersuchungen zur Abstammungsklärung und zur Identifizierung außerhalb der Strafverfolgung

Grundsatz

- (1) Zu Zwecken der Abstammungsklärung und der Identifizierung dürfen nur die dazu geeigneten und erforderlichen genetischen Untersuchungen (DNA-Identifizierungsmuster) durchgeführt werden. Diagnostische oder prädiktive Untersuchungen nach Krankheitsanlagen oder Merkmalen der betroffenen Person sind unzulässig. Abgesehen vom Merkmal Geschlecht sind unvermeidliche Überschussinformationen so früh wie möglich zu vernichten.
- (2) Die untersuchende Stelle hat selbst die Proben bei der betroffenen Person zu entnehmen und dies zu dokumentieren.
- (3) Die Proben sind zu vernichten, wenn die betroffene Person dies wünscht oder ein Gericht die Vernichtung anordnet, im Übrigen wenn die genetische Untersuchung durchgeführt ist. Die Dokumentation ist 10 Jahre aufzubewahren.

Einwilligung

Genetische Untersuchungen zu Zwecken der Abstammungsklärung oder Identifizierung dürfen nur mit schriftlicher Einwilligung der betroffenen Person oder ihres gesetzlichen Vertreters oder auf gerichtliche oder behördliche Anordnung durchgeführt werden. Für genetische Untersuchungen zur Abstammungsklärung bei Minderjährigen gilt § 1629 BGB.

Anordnung genetischer Untersuchungen zu Identifizierungszwecken

- (1) In gerichtlichen und Verwaltungsverfahren kann das Gericht bzw. die Verwaltungsbehörde eine genetische Untersuchung zu Identifizierungszwecken anordnen, wenn die Identität einer Partei, eines Beteiligten oder einer für das Verfahren wichtigen dritten Person oder Leiche in Zweifel steht und nicht auf andere Weise geklärt werden kann. Ist die Identitätsfeststellung Voraussetzung für die Gewährung von behördlichen Genehmigungen oder Leistungen an die betroffene Person, ist die genetische Untersuchung nur mit ihrer Einwilligung zulässig.

- (2) Die Anordnung hat die Art der Probe, das Ziel der Untersuchung sowie den Zeitpunkt der Vernichtung der Probe und der Löschung der genetischen Daten festzulegen. Bei lebenden Personen ist die Probe ohne Eingriff in die körperliche Unversehrtheit zu entnehmen, es sei denn, die betroffene Person willigt in einen Eingriff ein.

Genetische Untersuchungen zu Forschungszwecken

Konkrete, zeitlich befristete Forschungsvorhaben

- (1) Für konkrete, zeitlich befristete Forschungsvorhaben ist die genetische Untersuchung von Proben und die Erhebung, Verarbeitung und Nutzung genetischer Daten zulässig, wenn
1. die Proben und die genetischen Daten der betroffenen Person nicht mehr zugeordnet werden können oder
 2. im Falle, dass der Forschungszweck die Möglichkeit der Zuordnung erfordert, die betroffene Person nach den Anforderungen für Forschungsvorhaben eingewilligt hat (siehe unten) oder
 3. im Falle, dass weder auf die Zuordnungsmöglichkeit verzichtet, noch die Einwilligung eingeholt werden kann, das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schützenswerten Interessen der betroffenen Person überwiegt und der Forschungszweck nicht auf andere Weise zu erreichen ist.
- (2) In den Fällen der Ziffer (1) Nr.2 und 3 sind bei Proben vor der Untersuchung, bei genetischen Daten vor der Verarbeitung oder Nutzung die Merkmale, mit denen ein Personenbezug hergestellt werden kann, gesondert zu speichern. Die Zuordnungsmöglichkeit ist aufzuheben, sobald der Forschungszweck es erlaubt und schutzwürdige Interessen der betroffenen Person gemäß der Regelung über deren Rechte (siehe unten) nicht entgegenstehen.

- (3) Die Proben dürfen nur im Rahmen des Forschungsvorhabens untersucht, die genetischen Daten dürfen nur zu den Zwecken verarbeitet oder genutzt werden, für die sie im Rahmen des Forschungsvorhabens erhoben wurden.
- (4) Mit Beendigung des Forschungsvorhabens sind die Proben zu vernichten und die genetischen Daten zu löschen. Ist ihre Aufbewahrung oder Speicherung zum Zwecke der Selbstkontrolle der Wissenschaft erforderlich, ist dies in pseudonymisierter Form für einen Zeitraum von längstens 10 Jahren zulässig.
- (5) Konkrete, zeitlich befristete Forschungsvorhaben nach Ziffer (1) bedürfen der vorherigen Zustimmung der zuständigen Ethikkommission.

Sammlungen von Proben und genetischen Daten

- (1) Das Sammeln von Proben einschließlich isolierter DNS oder RNS oder von genetischen Daten zu allgemeinen Forschungszwecken ist nur zulässig, wenn die betroffenen Personen über Zweck und Nutzungsmöglichkeiten der Sammlung aufgeklärt wurden und in die Entnahme der Probe sowie die Aufnahme von Probe und Daten in die Sammlung eingewilligt haben (siehe unten). Satz 1 gilt entsprechend für die Übernahme bereits vorhandener Proben oder genetischer Daten.
- (2) Die Zuordnung der Probe und der genetischen Daten zur betroffenen Person ist vor der Aufnahme in die Sammlung aufzuheben. Erfordert der Zweck der Sammlung die Möglichkeit einer Zuordnung, sind die Proben und die genetischen Daten vor der Aufnahme in die Sammlung bei Treuhändern zu pseudonymisieren.
- (3) Vor einer Weitergabe von Proben und einer Übermittlung genetischer Daten für konkrete Forschungsvorhaben ist die Möglichkeit der Zuordnung zur betroffenen Person aufzuheben oder, wenn der Forschungszweck dem entgegensteht, eine weitere Pseudonymisierung gemäß den Regelungen bei Treuhändern (siehe unten) vorzunehmen.
- (4) Der Träger einer Sammlung hat eine kontinuierliche interne Datenschutzkontrolle sicherzustellen. Bei Trägerwechsel gehen alle Verpflichtungen aus diesem Gesetz auf den neuen Träger über. Soll eine Sammlung beendet werden, sind die Proben zu vernichten und die genetischen Daten sowie die beim Treuhänder (siehe unten) gespeicherten Daten zu löschen.

- (5) Die Einrichtung einer neuen und die Übernahme einer bestehenden Sammlung nach Ziffer (1) bedürfen der Zustimmung durch die zuständige Ethikkommission. Die Einrichtung ist mit dem Votum der Ethikkommission und unter Darlegung der in den Vorschlägen zur Sammlung von Proben und genetischen Daten, zur Aufklärung und Einwilligung, über die Rechte der betroffenen Person und über die Treuhänder geforderten Maßnahmen bei der für die Datenschutzkontrolle zuständigen Behörde anzuzeigen. Betriebs- und Geschäftsgeheimnisse sind kenntlich zu machen. Die Anzeige ist jeweils nach 5 Jahren mit einer Begründung der weiteren Speicherung zu erneuern. Ebenso sind die Vernichtung oder Löschung von Sammlungen nach Ziffer (1), die Löschung der Zuordnungsmerkmale bei Treuhändern und Trägerwechsel nach Ziffer (4) anzuzeigen.

Aufklärung und Einwilligung

- (1) Die betroffene Person ist vor ihrer Einwilligung im Falle, dass der Forschungszweck die Möglichkeit der Zuordnung erfordert (siehe oben), oder bei Sammlungen von Proben oder genetischen Daten (siehe oben) insbesondere aufzuklären über
- den verantwortlichen Träger des Forschungsvorhabens oder der Sammlung,
 - das Ziel der Forschung oder bei Sammlungen die möglichen Forschungsrichtungen,
 - ihre Rechte bei Patentanmeldungen und gewerblichen Nutzungen,
 - die Dauer der Aufbewahrung von Proben und der Speicherung der genetischen Daten,
 - Zeitpunkt und Art der Pseudonymisierung von Proben und genetischen Daten, sowie über die mögliche Wiederherstellung der Zuordnung zur betroffenen Person,
 - ihr Recht – vorbehaltlich der pseudonymisierten Verarbeitung nach Beendigung des Forschungsvorhabens (siehe oben) – die Vernichtung der Probe und die Löschung der genetischen Daten oder die Aufhebung der Zuordnungsmöglichkeit zu verlangen, wenn sie die Einwilligung widerruft,

- ihr Recht, Ergebnisse von Untersuchungen nicht zur Kenntnis zu nehmen oder unter Nutzung eines darzustellenden Ent-Pseudonymisierungsverfahrens zu erfahren,
- ihr Recht, Auskunft über die zu ihr gespeicherten genetischen Daten zu verlangen.

Die Aufklärung hat schriftlich und mündlich zu erfolgen.

- (2) Die Einwilligung soll die Entscheidung darüber umfassen, ob die betroffene Person vom Ergebnis der Untersuchung Kenntnis nehmen will oder nicht.
- (3) Die Einwilligung kann eine Schweigepflichtentbindung für zu benennende behandelnde Ärzte einschließen, wenn die betroffene Person über Art und Umfang der Patientendaten informiert wird, die der Arzt für das Forschungsvorhaben (siehe oben) oder die Sammlung von Proben oder genetischen Daten (siehe oben) übermittelt.

Rechte der betroffenen Person

- (1) Hinsichtlich der genetischen Daten stehen der betroffenen Person die im Bundesdatenschutzgesetz geregelten Rechte zu. Widerruft die betroffene Person ihre Einwilligung (siehe oben), sind entweder die Probe zu vernichten und die genetischen Daten zu löschen oder die Zuordnungsmerkmale zu löschen.
- (2) Erbringt ein Forschungsvorhaben Ergebnisse, die für die betroffene Person von Bedeutung sind, veranlasst der Träger des Forschungsvorhabens eine Unterrichtung der betroffenen Person. Dies gilt nicht, wenn die betroffene Person erklärt hat, von dem Untersuchungsergebnis keine Kenntnis nehmen zu wollen (siehe oben).

Treuhänder

- (1) Die Pseudonymisierung von Proben und genetischen Daten erfolgt durch einen Treuhänder. Er vergibt die Pseudonyme unverzüglich, verwahrt und verwaltet die Zuordnungsmerkmale und sichert die Rechte der betroffenen Person (siehe oben). Soweit erforderlich, kann er für diese Zwecke Kontakt mit der betroffenen Person aufnehmen. Er hat keinen Zugriff auf genetische Daten.
- (2) Treuhänder kann eine natürliche Person sein, die von Berufs wegen einer besonderen Schweigepflicht unterliegt und vom Träger des Forschungsprojekts

oder der Sammlung von Proben oder genetischen Daten unabhängig ist. Im Vertrag zwischen dem Treuhänder und dem Träger des Forschungsvorhabens oder der Sammlung von Proben oder genetischen Daten sind insbesondere die Anlässe und das Verfahren zur Wiederherstellung des Personenbezuges, die Nutzungsformen durch die Selbstkontrollgremien der Wissenschaft sowie die technischen und organisatorischen Maßnahmen zur Datensicherheit festzulegen. Der Vertrag ist vorab der für die Datenschutzkontrolle zuständigen Behörde vorzulegen.

Schlussvorschläge

Ordnungswidrigkeit

Ordnungswidrig handelt, wer

- eine Reihenuntersuchung ohne die erforderliche Zulassung durchführt oder
- den Anzeigepflichten bei der Einrichtung einer neuen oder der Übernahme einer bestehenden Sammlung von Proben oder genetischen Daten oder bei bestehenden Proben- oder genetischen Datensammlungen nicht fristgemäß nachkommt.

Straftaten

- (1) Wer genetische Testverfahren unter Verstoß gegen die Anforderungen an das Inverkehrbringen genetischer Tests und Angebote von genetischen Untersuchungen einführt oder in Verkehr bringt oder genetische Untersuchungen ohne eine individuelle Beratung öffentlich anbietet, wird mit bestraft. Handelt die Täterin oder der Täter gewerbsmäßig, ist die Strafe
- (2) Wer vorsätzlich oder fahrlässig eine genetische Untersuchung zu medizinischen Zwecken durchführt, ohne
 - Arzt oder Ärztin zu sein,
 - die für die genetischen Untersuchungen zu medizinischen Zwecken festgelegten Beschränkungen der Untersuchungszwecke einzuhalten,
 - die geforderte Aufklärung und Beratung unternommen bzw. sichergestellt zu haben oder

- die Einwilligung der betroffenen Person eingeholt zu haben,

wird mit bestraft.

(3) Wer als Arbeitgeber oder als Versicherer gegen das Verbot genetischer Untersuchungen verstößt, ohne dass die vorgesehene Ausnahmeregelung eingreift, wird mit bestraft.

(4) Wer vorsätzlich oder fahrlässig eine genetische Untersuchung zu Zwecken der Abstammungsklärung oder Identifizierung in unzulässiger Weise auf prädiktive oder diagnostische Ziele ausrichtet oder ohne die geforderte Einwilligung durchführt, wird mit bestraft.

(5) Wer vorsätzlich oder fahrlässig personenbeziehbare Proben, DNS-/RNS-Teile oder genetische Daten entgegen den Regelungen für genetische Untersuchungen zu Forschungszwecken

- ohne Einwilligung oder Aufklärung zu Forschungszwecken nutzt oder

- in Sammlungen für Forschungszwecke zur Verfügung stellt,

wird mit bestraft.

Antrag

Die oben aufgeführten Straftaten werden nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person und die für die Datenschutzkontrolle zuständige Behörde.

Befristung

Die Regelungen sind auf zehn Jahre zu befristen. Acht Jahre nach In-Kraft-Treten haben die für die Datenschutzkontrolle zuständigen Behörden unter Federführung des Bundesbeauftragten für den Datenschutz dem Gesetzgeber einen Bericht über die Wirksamkeit der vorgeschlagenen Regelungen und über neue Gefährdungen für das Persönlichkeitsrecht sowie zu möglichen Rechtsvereinfachungen vorzulegen. Diesem Bericht sind Stellungnahmen des Ethikrates und der Deutschen Forschungsgemeinschaft beizufügen.

Übergangsvorschrift

Träger von bestehenden Proben- und genetischen Datensammlungen haben der Anzeigepflicht bei der Einrichtung einer neuen oder der Übernahme einer bestehenden Sammlung innerhalb von sechs Monaten nach In-Kraft-Treten dieses Gesetzes nachzukommen. Innerhalb dieser Frist ist den Anforderungen an die Einwilligung zu entsprechen. Vor In-Kraft-Treten dieses Gesetzes ohne Einwilligung gewonnene Proben und erhobene genetische Daten sind spätestens nach zwei Jahren zu vernichten bzw. zu löschen. Dies ist der für die Datenschutzkontrolle zuständigen Behörde anzuzeigen.

8.

ABKÜRZUNGSVERZEICHNIS



ABMG	Autobahnmautgesetz für schwere Nutzfahrzeuge
AFIS	Automatisiertes Fingerabdruck-Identifizierungssystem
AfO	Interministerieller Ausschuss für Organisationsfragen
AK Medien	Arbeitskreis „Medien“ der Datenschutzbeauftragten des Bundes und der Länder
AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder
AmtsBl.	Amtsblatt
AO	Abgabenordnung
AZR	Ausländerzentralregister
BauGB	Baugesetzbuch
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Datenschutz
BGB	Bürgerliches Gesetzbuch
BGBI.	Bundesgesetzblatt
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtsgesetz
BMI	Bundesministerium des Innern
BND	Bundesnachrichtendienst
BOÄ	Berufsordnung der Ärztinnen und Ärzte
BR-Drs.	Bundesrats-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStU	Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BT-Drs.	Bundestagsdrucksache
BverfG	Bundesverfassungsgericht
BVerfGE	Entscheidung des Bundesverfassungsgerichts (Band ..., Seite ...)
BZRG	Bundeszentralregistergesetz
CAT	Centrum für Angewandte Telemedizin

DES	Data Encryption Standard (Kryptografisches Verfahren)
DFKI	Deutsches Forschungszentrum für Künstliche Intelligenz
DMZ	Demilitarisierte Zone
DSG	Datenschutzgesetz
DVZ M-V GmbH	Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
DWH	Data Warehouse
EG	Europäische Gemeinschaft
EG-DSRL	EG-Datenschutzrichtlinie
EGG	Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr
ELSTER	Elektronische Steuererklärung
EPOS	Elektronisches Personal-, Organisations- und Stellenverwaltungssystem
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
EVA	Elektronischer Vorgangsassistent
FAG	Fernmeldeanlagen-gesetz
GG	Grundgesetz
GPS	Global Positioning System
GUID	Globally Unique Identifier
GVOBl.	Gesetz- und Verordnungsblatt
HKR	Haushalts-, Kassen-, Rechnungswesen
Hundeh-VO	Hundealterverordnung
iGN M-V	Innovatives Gesundheitsnetz M-V
IHK	Industrie- und Handelskammer
IMA-IT	Interministerieller Ausschuss für Informationstechnik
IMEI	International Mobile Equipment Identification
IMSI	International Mobile Subscriber Identity

INPOL	Polizeiliches Informationssystem
InsO	Insolvenzordnung
IP	Internet Protokoll
IPSec	IP Security
ISDN	Integriertes Services Digital Network
ISO	Internationale Standardisierungsorganisation
IT	Informationstechnik
ITSEC	Information Technology Security Evaluation Criteria
KAN	Kriminalaktennachweis
KBA	Kraftfahrt-Bundesamt
LAN	Lokal Area Network (lokales Netz)
LAPIS	Landesweites Polizei-Informationssystem
LArchivG	Landesarchivgesetz
LAVINE	Landesverwaltungs- und Informationsnetz
LBG M-V	Landesbeamtengesetz Mecklenburg-Vorpommern
LKA	Landeskriminalamt
LKHG M-V	Landeskrankenhausgesetz Mecklenburg-Vorpommern
LKSt	Koordinierungs- und Beratungsstelle der Landesregierung für Informations- und Telekommunikationstechnik in der Landesverwaltung
LMG	Landesmeldegesetz für das Land Mecklenburg-Vorpommern
LverfSchG M-V	Landesverfassungsschutzgesetz Mecklenburg-Vorpommern
MAC	Medium Access Control
MDK	Medizinischer Dienst der Krankenversicherung
NAT	Network Address Translation
NDR	Norddeutscher Rundfunk
NDS	Network Directory System
NSM	Netz- und Systemmanagement
ÖGDG	Gesetz über den Öffentlichen Gesundheitsdienst

OSS	Open-Source-Software
OWI	Ordnungswidrigkeit
PAD-MV	Personenarbeitsdatei Mecklenburg-Vorpommern
PC	Personalcomputer
PED M-V	Polizeiliche Erkenntnisdatei Mecklenburg-Vorpommern
PERSYS	Personal- und Stellenverwaltungssystem
PGP	Prittx Good Privacy
PIN	Persönliche Identifikations-Nummer
PKG	Parlamentarisches Kontrollgremium
PKZ	Personenkennzahl
PROfiskal	HKR-Verfahren
PSN	Processor Serial Number (Prozessoriennummer)
RSA	Kryptographisches Verfahren (Rivest, Shamir, Adlemaan)
SGB I	Sozialgesetzbuch Erstes Buch
SGB IV	Sozialgesetzbuch Viertes Buch
SGB V	Sozialgesetzbuch Fünftes Buch
SGB VIII	Sozialgesetzbuch Achstes Buch
SGB X	Sozialgesetzbuch Zehntes Buch
SGB XI	Sozialgesetzbuch Elftes Buch
SigG	Signaturgesetz
SigV	Signaturverordnung
SOG M-V	Gesetz über die öffentliche Sicherheit und Ordnung Mecklenburg-Vorpommern
StPO	Strafprozessordnung
StVÄG	Strafverfahrensänderungsgesetz
StVG	Straßenverkehrsgesetzes
TDDSG	Telekommunikations-Datenschutzgesetz
TDSV	Telekommunikations-Datenschutzverordnung
TK	Telekommunikation

TKG	Telekommunikationsgesetz
TKÜV	Telekommunikationsüberwachungsverordnung
TV	Television
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UMTS	Universal Mobile Telecommunication System
VNC	Virtual Network Computing
VPN	Virtuelles Privates Netz
WAN	Wide Area Network (Weitverkehrsnetz)
WEP	Wired Equivalent Privacy
WLAN	Wireless Lokal Area Network
WWW	World Wide Web
ZEVIS	Zentrales Verkehrsinformationssystem

9.

STICHWORTVERZEICHNIS



A Abhören	17
Abschottung	67
ActiveX	128
Adresse	152
AfO	125
Akteneinsichtsrecht	98
akustische Wohnraumüberwachung	25
Amt	67
Amts- oder besonderes Berufsgeheimnis	136
amtsfreie Gemeinde	67
Anamnese	95
Anhalte- und Sichtkontrolle	154
Antivirensoftware	130
Arbeitgeber	79
Arbeitnehmer	79
Arbeitskreis "Technische und organisatorische Datenschutzfragen"	129, 139, 141, 158
Arbeitskreis Medien	130
Arbeitskreis Statistik und Wahlen	67
Arbeitsorganisation	135
Arbeitspapier	151
Arbeitsplatz	129
Arbeitszeitverordnung	135
Archivgut	111
ärztliche Berufspflicht	86
ärztliche Schweigepflicht	99, 112
Asylverfahrensgesetz	39
Auftragsdatenverarbeitung	148, 153
Aufzeichnung	104
Ausbildungsplatzförderung	114
Auskunft	152
Auskunftsrecht	98
Auskunftssperre	57, 152
Ausländer	40
Ausländergesetz	39
Ausweispapiere	154
Autobahnbenutzungsgebühr	52
Autobahnmautgesetz	52
AZVO	135
Bauaufsichtsbehörde	68

B Bauherr	68
Beanstandung	66, 76, 83
Befragung	151
behördlicher Datenschutzbeauftragter	31
Belehrung	38
berechtigtes Interesse	22
Berichtspflicht	24
Berufs- und Amtsgeheimnis	17
Berufsausbildungsverhältnisse	114
Berufsordnung für die Ärztinnen und Ärzte in Mecklenburg-Vorpommern	98
Beschuldigte	37
Besitzer- und Herkunftsdaten	119
Bestandsdaten	71
Besteuerungsgrundlagen	75
Bevölkerungsbefragung	151
Bewegungsprofil	53
Beweismittel	82
Bewohner	151
Bilderkennung	144
Bildspeicher	145
Bildungsministerium	108
Biometrie	39
biometrische Merkmale	18, 19, 39
biometrische Verfahren	144
Briefgeheimnis	28
BSE	119
BSI	133, 139
Bundesamt für Sicherheit in der Informationstechnik	74, 133, 139
Bundesanstalt für Arbeit	152
Bundesbeauftragter für die Stasi-Unterlagen	83
Bundesdatenschutzgesetz	29, 53
Bundeskriminalamt	38
Bundesministerium des Innern	29
Bundesministerium für Wirtschaft	69
Bundesnachrichtendienst	27, 39
Bundesregierung	80
Bundeswahlgesetz	153
Bundeszentralregister	105
BundOnline 2005	124
Bürgerbüro	121

Bürgermeister	62
C Call-by-Call	156
Call-Center	122
Chipkartentechnik	158
Common Criteria	139
Cookie	127
Corporate Network	133
Cyber-crime-Konvention	72
D Data Warehouse	139, 150, 158
Datenerhebung	55, 81
Datengeheimnis	76
Datenkatalog	152
Datennetzkriminalität	72
Datenschutz- und Datensicherheitskonzept	66
Datenschutzaudit	29
datenschutzfreundliche Technologien	140, 151
Datenschutzniveau	73
Datenschutzrichtlinie	30
Datensparsamkeit	29, 53, 72
Datensparsamkeitsprinzip	127
Datenübermittlung	62, 106, 120
Datenverarbeitung	115
Datenverarbeitung im Auftrag	92, 98
Datenvermeidung	29
Deutsches Forschungszentrum für Künstliche Intelligenz	140
DFKI	140
Diebstahl	66
Dienstanweisung	36, 67, 149
Diensteanbieter	127
Dienstvereinbarung	129, 136
digitale Signatur	75, 122
Digitale Signatur	139
Diplomarbeit	163
Disease-Management-Programm	89
Disziplinarrecht	38
Disziplinarverfahren	36, 64
D-Kanal-Filter	133
DVZ M-V GmbH	125

E		
E-Commerce	139
EG	30
EG-Datenschutzrichtlinie	29
EG-Datenschutzverordnung	30
EGG	124
E-Government	124, 126
Eigentümer	151
Einer-für-Alle-Prinzip	125
Eingabekontrolle	34
Einkommensteuergesetz	80
Einkünfte	82
Einschulungsuntersuchung	94
Einwilligung	57, 91, 96, 97, 135
Einwilligungserklärung	114
Einwohner	152
Einzelbindungsnachweis	79
elektronische Signatur	124
Elektronische Steuererklärung	74
elektronische Unterschrift	75, 148
elektronischer Geschäftsverkehr	70
elektronischer Rechtsverkehr	123
elektronischer Verzeichnisdienst	128
Elektronischer Vorgangsassistent	33
Elektronisches Grundbuch	148
Elektronisches Personal-, Organisations- und Stellenverwaltungssystem	33
ELSTER	74
E-Mail	69, 129, 158
E-Mail-Adresse	127
Entschließung	29, 69, 70, 73, 150, 152
EPOS	33
Erhebung	67, 68, 151
Erhebungsbogen	95
Erlass	68
Ermittlung	72
Ermittlungsverfahren	38
EU	32, 73
EU-Grundrechte-Charta	32
Europäische Signaturrechtlinie	122
Europäischer Datenschutzbeauftragter	31
Europäischer Gerichtshof	31, 32

Europäischer Rat	32
Europarat	72
EVA	33
Evaluation	112, 141
Evaluierung	69
F	
Fachkonferenz	144
Fachschule	163
Fahndungsausschreibung	37
Fahndungsmethode	41
Fahrzeug	154
Fernmeldegeheimnis	28, 35, 70, 73
Fernsehen	22
Fernsehkabelnetz	69
Finanzbehörde	79
Finanzministerium	79
Fingerabdruck	18, 39
Firewall	108, 127, 130
Flatrates	80
flexible Arbeitszeit	135
Flughafen	106
Fortbildung	163
Fragebogen	152
Fremdenverkehrsabgabe	75
G	
G 10-Gesetz	27
G 10-Kommission	28
Gebäude	151
Gefahrenabwehr	155
Gemeinde	62, 150, 151
Gemeindevertretung	61
Geschäftsverteilungsplan	127
Gesichtsgeometrie	39
Gesundheitsdaten	86
Gesundheitsfürsorge	94
Gesundheitsnetz	91
Gesundheitsreform 2000	139
Gesundheitsvorsorge,	98
GPS	52
Großer Lauschangriff	17, 24, 155

Grundbuch	148
Grundgesetz	19
Grundrecht	32
Grundschatz	133
Gutachten	29

H Halterauskünfte	36
Handflächenabdruck	39
Handvenenmuster	39
Hausarzt	84
häusliche Gewalt	155
Heilbehandlung	86
Heimarbeitsplatz	135
Hilfsmittel	86
Hochbaustatistik	68
Hochschulbibliothek	111
Hochschule	112, 163
Hochschule Wismar	163
Homepage	126
https-Protokoll	74
Hundehalterverordnung	76
Hundesteuerdaten	77

I Identifikation	144
Identität	154
IMA IT	125, 151
IMSI-Catcher	18
informationelle Gewaltenteilung	121
informationelle Selbstbestimmung	16, 17, 19
Informationszugangsrecht	19
infrastrukturelle Sicherungsmaßnahmen	135
Innenminister	38
Innenministerium	152
INPOL-neu	34, 153
Insolvenzverfahren	25
Integrität	136
Interministerieller Ausschuss für Informations- und Kommunikationstechnik	125
Interministerieller Ausschuss für Organisationsfragen	125
Internet	22, 25, 26, 57, 69, 71, 73, 79, 108, 121, 129, 158
Internetangebot	129, 164

Interventionsstelle	155
Interviewer	152
Intranet	129, 159
IP-Nummer	127
Irismuster	39
IT-Strukturrahmen	33

J Java	128
---------------	-----

K Kennzeichnung	28
Kinder- und Jugendgesundheitsdienst	95
kommunale Statistikstelle	67
Kommunalstatistik	67
Kommunalwahlgesetz	153
Kommune	67, 68, 151
Kommunikationsadresse	128
Kontroll- und Informationsbesuch	67
Kontrollbehörde	19
Koordinierungs- und Beratungsstelle der Landesregierung	125, 141
Körpermerkmal	39
Krankenhausaufnahmevertrag	97
Krankenhausentlassungsbericht	93
Krankenkasse	94
Krankenversicherung	89
Krebsregister	95
kreisfreie Stadt	67
Kreistag	65
Kryptographie	125, 140, 158
kryptographisches Verfahren	74, 124
Kunsturhebergesetz	116

L Landesarchivgesetz	112
Landesdaten	153
Landeskrankenhausgesetz	98
Landesregierung	129
Landesstatistikgesetz	67
Landesverfassungsschutzgesetz	55

Landesveterinärämmt	119
Landeswahlgesetz	153
Landkreis	67
Landtag	25
Landwirt	119
landwirtschaftlicher Betrieb	119
LAPIS	33
Lauschangriff	24
LAVINE	78
Lehrevaluation	112
LKHG	98
LKSt	125, 141
LKW-Maut	52
Löschung	156

M Maut	52
Max-Planck-Institut	70
Medien	70, 119
Mediendienste	70, 73
Medienordnung	70
medizinische Informationssysteme	158
Meinungsfreiheit	70
Meldebehörde	151, 152
Meldedatenübermittlung	72
Melderechtsrahmengesetz	57
Melderegister	148, 152, 153
Melderegisterauskunft	57
Menschenrecht	19
Missbrauch	130
Mitarbeiter	129
Mitarbeiterdaten	126
mobile Informationstechnik	158
Mobilfunk	52
Mobiltelefon	18
Müllcontainer	37
Multimediainitiative	91

N Nachrichtendienste	71
nachrichtendienstliche Mittel	56
nichtöffentliche Sitzungen	63

nichtöffentlicher Bereich	120
Norddeutscher Rundfunk	71
Notfallplan	134
Novellierung	16, 29, 55
Nutzungsdaten	71, 73

O öffentliche Stellen	151
öffentlicher Dienst	105
Öffentlicher Gesundheitsdienst	98
Öffentlichkeitsfahndung	22
Online-Datenschutz-Prinzipien	127
Open Source	141, 158
Open-Source-Software	141
Ordnungswidrigkeiten	71
Ordnungswidrigkeitenverfahren	50
Organisationskontrolle	135
Orientierungshilfe	128, 130, 136
Orientierungshilfe Internet	158
OSS	141
Outsourcing	98
OWI	33

P Parlamentarische Kontrolle	24
Pass	18, 19
Passgesetz	39
Patientendaten	91
Patientendatenschutz	163
PC	80, 129
PED	33
Personalakte	102
Personalaktendatenverarbeitung	33
Personalausweis	18, 19
Personalausweisgesetz	39
Personaldaten	101, 106
Personalgespräch	104
Personenkennzahl (PKZ)	18
Personenkennzeichen	18
Persönlichkeitsrecht	22
PERSYS	108
Pflegekasse	86

Polizei	39, 101
Polizeiakten	37
Polizeidaten	155
Polizeidirektion	34, 37
Polizeistation	37
Postgeheimnis	28
Praktikum	163
privat	129
Privatanschrift	127
Privatgeheimnis	38
Privatsphäre	70
PROfiskal	77, 108
Protection Profiles	139
Protokolldaten	130
Protokollierung	33, 36, 109, 129
pseudonymisierte Daten	89
Pseudonymisierung	139
R Rasterfahndung	17, 41
Rechnung	156
Rechnungsprüfung	64, 65
Recht auf informationelle Selbstbestimmung	56
rechtsextremistisch	55
Rechtshilfe	73
Rechtsschutzgarantie	56
Register	151
Retinamuster	39
Revision	133, 140, 163
Revisionskonzept	133
Revisionsicherheit	33
Risikostrukturausgleich	89
RSA	74
Rundfunk	70
Rundfunkgebührenfinanzierung	71
S Satellitennavigationssystem	52
Satzung	113
Schlachthof	119
Schläfer	42
Schleierfahndung	17, 154
Schriftform	123

Schriftgut	37
Schulung	163
Schutzfristen	112
Schweigepflicht	84
Sicherheits- und Ordnungsgesetz	154
Sicherheitsbehörden	156
Sicherheitskonzept	133
Sicherheitsüberprüfungsgesetz	40
Signatur	57
Signaturgesetz	122
Signaturverordnung	122
SOG M-V	154
Sozialdaten	43
Sozialdatenschutz	163
sozialer Status	88
Sozialhilfebescheid	88
Sozialhilfeempfänger	81, 88
Sozialleistungsträger	81
Sparkasse	116, 117
Staatsanwalt	149
Staatsanwaltschaft	37
Statistik	67
Statistikamt	152
Statistikgeheimnis	152
statistische Erhebungsstelle	68
statistische Geheimhaltung	67
Statistisches Bundesamt	152
Statistisches Landesamt	67, 68, 152
Steuergeheimnis	77
steuerpflichtig	79
Stichprobe	151
Strafverfahrensänderungsgesetz	22
Strafverfolgung	71
Strafverfolgungsbehörde	22
Straßenbenutzungsgebühr	52, 158
Stromleitung	69
T TDDSG	127
TDG	127
Technikregelungen	29

technische und organisatorische Maßnahmen	66
Telearbeit	135, 163
Teledienst	70, 73, 127
Teledienstedatenschutzgesetz	71, 124, 127
Teledienstegesetz	124, 127
Telefon	79
Telefongebühren	156
Telefonnummer	79
Telefonüberwachung	70
Telefonverzeichnis	127, 128
Telekommunikation	69, 70
Telekommunikations-Datenschutzrichtlinie	156
Telekommunikations-Datenschutzverordnung	155
Telekommunikationsgeheimnis	79
Telekommunikations-Überwachungsverordnung	69
Telemedizin	158, 163
Terroranschlag	41
Terrorismus	39
Terrorismusbekämpfung	19
Terrorismusbekämpfungsgesetz	17
Testerhebung	151
Tierseuchenmeldung	119
TK-Anlage	133
TK-Datenschutzrichtlinie	30
TK-Unternehmen	156
Todesfall	37
Transparenz	140
Trennungsgebot	39
Triple-DES	74
Trojanisches Pferd	141
Trustcenter	125

U Überarbeitung des Datenschutzrechts	16
Übermittlung	73, 75
Überwachung	69
Überwachungsinfrastruktur	144
Überwachungsmaßnahme	18
Überwachungsstaat	19
Überwachungstechnik	144

Umsetzung der europäischen Datenschutzrichtlinie	16
Unfallversicherungsträger	85
Universität	112
Universität Greifswald	163
Universität Rostock	163
unmittelbare Gefahr	120
USA	41

V Verbindungsdaten	73, 156
Verbunddaten	153
verdachts- und ereignisunabhängige Personenkontrolle	154
Verfassungsschutzbehörde	39
Verfolgung	72
Verifikation	144
Verkehrsüberwachung	50
Veröffentlichung	62
Verschlüsselung	71, 74, 109, 124, 125, 130, 134, 139, 145
Verschweigerecht	105
Verschwiegenheitspflicht	62, 65, 76
Vertragsverhandlungen	117
Vertraulichkeit	70, 136
Vertriebene	83
Vertriebenenzuwendung	83
Vertriebenenzuwendungsgesetz	83
Verwaltung	129
Verwaltungsreform	121
Verwaltungsregister	151
Verwaltungsverfahrenrecht	123
Verwaltungsvollzug	68
Verwertungsverbot	106
Verzeichnisdienst	159
Videoaufzeichnungen	50
Videokamera	115, 143
Videoüberwachung	19, 143, 163
Virtuelles Datenschutzbüro	164
Völkerverständigung	55
Volkszählung	151
Volkszählungsurteil	19
Vorkaufsrecht	150
Vorladungen	37

Vorratsspeicherung	156
Vortrag	163
VPN	109
W Wählerverzeichnis	148, 152
Wahlrechtsausschluss	148
Website	79
Widerspruchsrecht	57
Wohnung	155
Wohnungsgesellschaft	115
Z Zensustestgesetz	151
Zentrales Verkehrsinformationssystem	34
Zentralstelle	38
Zertifikat	124
Zertifizierung	74, 141
Zeuge	22
Zeugenanhörung	37
Zeugin	22
Zeugnisverweigerungsrecht	99
ZEVIS	34, 36
Zivilprozessordnung	123
Zoomfunktion	145
Zugang	31, 32
Zwangsaufzeichnung	35
Zwangsversteigerungen	26
Zweckbindung	22, 53, 61

10.

PUBLIKATIONEN

Beim Landesbeauftragten für den Datenschutz sind derzeit folgende Publikationen kostenlos erhältlich bzw. stehen im Internetangebot unter [www.lfd.m-v.de] zum Abruf bereit:

- **Gesetze und Verordnungen zum Datenschutz** - Stand 2001 - (Loseblattsammlung)
- **Technik und Datenschutz** - Stand 1996 - (Arbeitsergebnisse und Tagungsunterlagen des Arbeitskreises Technik - Broschüre)
- **Datenschutzfreundliche Technologien** - Stand 1998 - (Broschüre)
- **Vom Bürgerbüro zum Internet – Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung** - Stand 2000 - (Broschüre)
- **Handys - Komfort nicht ohne Risiko** - Stand 1998 - (Faltblatt)

Tätigkeitsberichte (in Broschürenform)

- 1. Tätigkeitsbericht für den Zeitraum 1992/93
- 2. Tätigkeitsbericht für den Zeitraum 1994/95
- 3. Tätigkeitsbericht für den Zeitraum 1996/97
- 4. Tätigkeitsbericht für den Zeitraum 1998/99
- 5. Tätigkeitsbericht für den Zeitraum 2000/01

Informationen zum Datenschutz

(Faltblätter mit aktuellen Informationen)

- 2. Datenschutz und Personalcomputer - Stand 1992
- 5. Datenschutz und Verfassungsschutz - Stand 1993
- 6. Datenschutz und Personen-Identifikation - Stand 1993 -
- 7. Datenschutz und Telefax - Stand 1993 -
- 9. Datenmissbrauch - Stand 1993 -
- 12. Das ISDN-Netz - Stand 1994 -
- 13. Freiwillige Patienten-Chipkarten - Stand 1994 -
- 15. Umgang mit Sozialdaten - Stand 1995 -
- 16. Personenbezogene Daten in der Forschung - Stand 1995 -

- | | |
|--|----------------|
| 17. Technikfolgenabschätzung | - Stand 1995 - |
| 18. Sicherheit der Informationstechnik | - Stand 1995 - |
| 19. Personalakten und Personalaktendaten | - Stand 1995 - |
| 20. Statistische Erhebungen | - Stand 1995 - |

Handreichungen (Kopien)

- Hinweise zu den Aufgaben eines internen Datenschutzbeauftragten öffentlicher Stellen - Stand 1992 -
- Orientierungshilfe „Forderung an Wartung und Fernwartung von DV-Anlagen“ - Stand 1993 -
- Hinweise zur Führung von Dateibeschreibung und Geräteverzeichnis - Stand 1993 -
- Organisationshilfe zur Vernichtung von Schriftgut - Stand 1996 -
- Orientierungshilfe „Datenschutzrechtliche Protokollierung beim Betrieb informations-technischer Systeme (IT-Systeme)“ - Stand 1994 -
- Orientierungshilfe „Datenschutzrechtliche Aspekte beim Einsatz optischer Datenspeicherung“ - Stand 1995 -
- Orientierungshilfe „Anforderungen zur informationstechnischen Sicherheit bei Chipkarten“ - Stand 1996 -
- Musterdienstvereinbarung über die Nutzung der Telekommunikationsanlage - Stand 1998 -
- Empfehlungen zur Passwortgestaltung und zum Sicherheitsmanagement - Stand 1991 -
- Orientierungshilfe Telearbeit - Stand 2000 -

Informationen des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz (Broschüren) [<http://www.bfd-bund.de>]

- BfD - INFO 1 - Bundesdatenschutzgesetz - Stand 1996 -
(vergriffen, Neuauflage geplant)
- BfD - INFO 2 - Der Bürger und seine Daten - Stand 1993 -
- BfD - INFO 3 - Schutz der Sozialdaten - Stand 1994 -
- BfD - INFO 4 - Der behördliche Datenschutzbeauftragte - Stand 1996 -
- BfD - INFO 5 - Datenschutz und Telekommunikation - Stand 1998 -
(vergriffen, Neuauflage geplant)

