BREMISCHE BÜRGERSCHAFT **Drucksache 16 /1362**
Landtag 31. 03. 07
16. Wahlperiode

29. Jahresbericht des Landesbeauftragten für Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats über das Ergebnis der Tätigkeit im Jahre 2006 den 29. Jahresbericht zum 31. März 2007 (§ 33 Abs. 1 Bremisches Datenschutzgesetz – BremDSG). Redaktionsschluss für die Beiträge war der 31. Dezember 2006.

Sven Holst
Landesbeauftragter für Datenschutz und Informationsfreiheit

Inhaltsverzeichnis

1. Vorwort

Das Berichtsjahr 2006 ist geprägt von zwei Besonderheiten, die über die allgemeinen Aufgaben des Landesbeauftragten hinausgehen: Mir fiel der Vorsitz bei den obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich zu (vgl. Ziff. 18.1 dieses Berichts) und mir wurden die Beratungs- und Kontrollaufgaben nach dem Bremer Informationsfreiheitsgesetz (BremIFG) übertragen, die ebenfalls mit einer Berichtspflicht verbunden sind. Die parlamentarischen Beratungen zum BremIFG und die ersten Schritte zur Umsetzung hatten Vorrang für mich, denn Fehlentwicklungen am Anfang muss man meistens teuer bezahlen. Es lag mir also daran, mehr als das Notwendige zu tun, um das Informationsfreiheitsgesetz in gutes Fahrwasser zu bringen. Da mir hierfür in 2006 kein zusätzliches Budget zur Verfügung gestellt wurde, gingen die Aktivitäten für die Informationsfreiheit zu Lasten des Datenschutzes. Auch der Konferenzvorsitz bei den Datenschutzaufsichtsbehörden verpflichtete mich, neben organisatorischen Aufgaben mehr als sonst alle Datenschutzangelegenheiten im privaten Sektor intensiv zu begleiten, um einen reibungslosen und effektiven Ablauf der beiden Sitzungen in Bremerhaven und Bremen sicherzustellen. Die Ergebnisse und das Feedback der Teilnehmer von Bund und Ländern zeigen, dass sich diese Investition gelohnt hat. Neben den Aufgaben nach dem Informationsfreiheitsgesetz stehen meiner Dienststelle seit Mitte des Jahres weitere neue Belastungen ins Haus: Leider hat sich der Bundesgesetzgeber in 2006 dazu entschieden, mit dem Gesetz zum Abbau bürokratischer Hemmnisse (vgl. Ziff. 18.7 dieses Berichts), auch Mittelstandsentlastungsgesetz genannt, die Regelungen über die Bestellung betrieblicher Datenschutzbeauftragter so zu verändern, dass ich den kleineren und mittleren Unternehmen vermehrt in Datenschutzfragen Hilfestellung leisten muss. Es hat also eine Verlagerung von Aufgaben auf die Datenschutzaufsichtsbehörden der Länder gegeben, die Entlastung der Wirtschaft ist in Teilen durch Belastung des Staates erkauft worden.

Wegen des über die Jahre ständig zunehmenden Einsatzes von elektronischer Kommunikation und Datenverarbeitung und der Erweiterung der Aufgaben meiner Dienststelle bei gleichzeitigem Abbau von Personal bin ich längst schon nicht mehr in der Lage, allen an mich herangetragenen Anforderungen Rechnung zu tragen. Deshalb ist es notwendig, Schwerpunkte zu setzen. Ein Schwerpunkt wird in 2007 die Verlagerung weiterer Teile der elektronischen Datenverarbeitung des Landes Bremen zu Dataport sein (vgl. Ziff. 15.1 dieses Berichts). Dataport ist eine gemeinsame Anstalt öffentlichen Rechts der Länder Bremen, Hamburg, Mecklenburg-Vorpommern und Schleswig-Holstein und wird für diese Länder in unterschiedlichem Umfang als IT-Dienstleister tätig. Mit Gesetz vom 20. Dezember 2005 ist das Land Bremen dem Länderstaatsvertrag zur Errichtung von Dataport beigetreten (Brem.GBl. 2005, S. 615, vgl. 28. JB, Ziff. 15.2). Mit Gesetz vom 19. Dezember 2006 wurde zum 1. Januar 2007 die bremische Niederlassung von Dataport durch Überleitung des Eigenbetriebs Fidatas Bremen gegründet (Brem.GBl. 2006, S. 544). Mitte 2006 begannen die intensiven Beratungen hierzu, die damit einhergehenden datenschutzrechtlichen Fragen wurden von mir begleitet. In 2007 nun steht u. a. die Portierung sämtlicher DV-Verfahren des Bremer Rechenzentrums ID Bremen an. Dieser Prozess bedeutet natürlich auch eine neue Herausforderung für das Technikteam in meinem Hause. Da es sich bei Dataport um ein gemeinsames Rechenzentrum der genannten vier Länder handelt, kommt neben der räumlichen Entfernung für Prüfungen im Rechenzentrum in Schleswig-Holstein auch noch ein weiterer Abstimmungsbedarf mit den Datenschutzbeauftragten der anderen Länder hinzu. In jedem Fall bedarf der Start intensiver Zusammenarbeit, die ohne den Wechsel nicht entstanden wäre. Andererseits erwarte ich durch die Zusammenarbeit auch Effektivitätssteigerungen. Es bleibt also abzuwarten, zu welcher Seite sich die Waage langfristig neigen wird.

Erstmalig in diesem Jahr wurde die Auditierung eines Verfahrens nach § 7 b des Bremischen Datenschutzgesetzes eingeleitet (vgl. Ziff. 3.1 dieses Berichts). Öffentliche Stellen können nach dieser Vorschrift zur Verbesserung des Datenschutzes und der Datensicherheit ihre Verfahren sowie ihre technischen Einrichtungen durch einen unabhängigen Gutachter prüfen und bewerten lassen (Auditierung). Ziel des Datenschutzaudits ist die Verbesserung des Datenschutzes und der Datensicherheit. Nach erfolgreichem Abschluss sind die Stellen berechtigt, ein Datenschutzgütesiegel zu führen. Wer sich in der Weise um einen hohen Datenschutzstandard im eigenen Hause bemüht, hat dann verdient, dass er dieses Engagement mit einem Gütesiegel seinen Kunden gegenüber zum Ausdruck bringen kann. Ich kann nur dazu auffordern, mehr von dieser Möglichkeit Gebrauch zu machen.

Ausführliche datenschutzrechtliche Stellungnahmen im Rahmen der Gesetzgebungsberatung habe ich insbesondere zu folgenden Gesetzentwürfen des Landes abgegeben: Bremisches Meldegesetz, Bremisches Hochschulreformgesetz, Bremisches Schuldatenschutzgesetz und Bremisches Verfassungsschutzgesetz.

1.1 Die obersten Datenschutzaufsichtsbehörden kommen in Bremen zusammen

Die Vertreter der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich (der so genannte Düsseldorfer Kreis) tagten im Berichtsjahr im Land Bremen, die Frühjahrssitzung fand in Bremerhaven, die Herbstsitzung in Bremen statt. Ich durfte den Vorsitz in dem Gremium führen, was natürlich neben einer intensiven Vorbereitung der Themen mit der Protokollführung, der Pressearbeit und der Vermittlung der Ergebnisse gegenüber der Wirtschaft und ihren Verbänden verbunden ist. Bei der Ausgestaltung des Rahmens haben mich in Bremen der Präsident der Bürgerschaft und in Bremerhaven der Oberbürgermeister tatkräftig unterstützt und so zu einem guten Gelingen der Sitzungstage beigetragen. Neben der Behandlung vieler Einzelfragen (vgl. Ziff. 18.1 dieses Berichts) möchte ich zwei auf der Herbstsitzung in Bremen verabschiedete Beschlüsse hervorheben. Der eine formuliert Voraussetzungen für den datenschutzgerechten Einsatz der Mikrochip-Technologie RFID (vgl. Ziff. 18.2 dieses Berichts), der andere betrifft die Behandlung von Bankdaten im internationalen Zahlungsverkehr durch SWIFT (Society for Worldwide Interbank Financial Telecommunication); eine genauere Darstellung findet sich unter Ziffer 18.3 dieses Berichts. Nicht unerwähnt lassen möchte ich, dass es in der Frühjahrssitzung in Bremerhaven gelungen ist, verbindliche Regelungen aufzustellen, die eine Veröffentlichung der Beschlüsse des Düsseldorfer Kreises erlauben. Dieser Schritt war aus meiner Sicht längst überfällig, auch wenn es wieder ein Stück mehr Arbeit bedeutet. Die Zusammenkunft der Vertreter der obersten Aufsichtsbehörden wurde auch genutzt, um sich aus erster Hand von kompetenten Informatikern und Juristen über neueste Entwicklungen informieren zu lassen. In Bremerhaven nutzte die datenschutz nord GmbH die Gelegenheit, ihre speziellen für den Datenschutz im Internet entwickelten Software-Prüftools vorzustellen. In Bremen stellten Vertreter des Chip-Herstellers Intel ihre Überlegungen bei der Weiterentwicklung von Prozessoren vor und berichteten dann über ihre TET („Trusted Execution Technology"), eine Technologie, um hardwareunterstützt Schutzstandards im Bereich der Identifikation und der Datensicherheit umzusetzen. Technologische Basis hierfür ist ein „Trusted Platform Module" (TPM), dass in die Chipsätze auf Motherboards integriert werden soll. Unabhängig von damit verbundenen Datenschutzfragen ist feststellbar, dass, ebenso wie zum Beispiel bei der Firma Microsoft, die in der Vergangenheit liegenden öffentlichen Reaktionen auf datenschutzunfreundliche technische Ausgestaltung (vgl. 25. JB, Ziff. 2.5 und 22. JB, Ziff. 18.4) ihre Wirkung gezeigt und zu einem Umdenken in diesen Unternehmen geführt haben.

1.2 Vertragsverletzungsverfahren vor dem EuGH

Im 28. Jahresbericht (vgl. Ziff. 3.1) hatte ich über das von der Europäischen Kommission am 5. Juli 2005 eingeleitete Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland wegen Verstoßes gegen Artikel 28 Abs. 1 Satz 2 der Richtlinie 95/46/EG (EG-Datenschutzrichtlinie) berichtet. Die Europäische Kommission vertritt die Auffassung, die derzeitigen Organisations- und Aufsichtsstrukturen der für die Überwachung der Datenverarbeitung im nicht öffentlichen Bereich zuständigen Kontrollstellen in den Ländern seien nicht mit Gemeinschaftsrecht vereinbar, da die verschiedenen Formen von Fach-, Rechts- und Dienstaufsicht nicht den Anforderungen der verlangten „völligen Unabhängigkeit" im Sinne des Artikel 28 Abs. 1 Satz 2 der Richtlinie 95/46/EG entsprechen.

Im Laufe dieses Jahres gab es Gespräche zwischen der Europäischen Kommission und der Bundesregierung mit dem Ziel, eine außergerichtliche Lösung herbeizuführen. Diese steht weiter aus. Die EU-Kommission hat daher mit Schreiben vom 15. Dezember 2006 (SG[2006]D/207794) eine mit Gründen versehene Stellungnahme (Nr. 2003/4820) gemäß Artikel 226 des Vertrags zur Gründung der Europäischen Gemeinschaft an die Bundesrepublik Deutschland übermittelt. Darin wird die Bundesrepublik Deutschland aufgefordert, binnen zwei Monaten der Stellungnahme nachzukommen und die völlige Unabhängigkeit der für die Datenverarbeitung nicht öffentlicher Stellen zuständigen Aufsichtsbehörden sicherzustellen. Parallel zu dem Fortgang des Vertragsverletzungsverfahrens dauern die Gespräche an. Im Zusam-

menhang dieser Gespräche hielt es das Bundesministerium des Innern in seiner Stellungnahme für unabdingbar, die Datenschutzaufsichtsbehörden für den nicht öffentlichen Bereich einer Rechtsaufsicht durch die Landesregierung oder durch eine oberste Landesbehörde zu unterwerfen. Meine Rechtsauffassung zur Situation in Bremen habe ich im 28. Jahresbericht (vgl. Ziff. 3.1) dargelegt, der Rechtsausschuss der Bürgerschaft ist unterrichtet, Aufsichtsmaßnahmen gegenüber der Datenschutzaufsichtsbehörde des Landes hat es in Bremen nicht gegeben.

1.3 Zur Entwicklung des Datenschutzes auf internationaler und auf Bundesebene

Auf eine Darstellung der Entwicklung des Datenschutzes auf internationaler und auf Bundesebene habe ich im Hauptteil des Berichts weitgehend verzichtet. An dieser Stelle jedoch möchte ich kurz darauf eingehen. Ein zentrales Thema der Sicherheitspolitik war die Terrorismusgefahr. Auf internationaler Ebene stand nach der Entscheidung des Europäischen Gerichtshofes (EuGH) vom 30. Mai 2006 die Überarbeitung des Abkommens zum Abruf der Fluggastdaten von den USA (Ministerium für Heimatschutz) an. Leider hat auch das zweite Abkommen vom Oktober 2006 für den Schutz der Fluggastdaten nur wenig gebracht. Das Pull-Verfahren bleibt zunächst bestehen (vgl. hierzu auch den 27. JB, Ziff. 15.2), auch die weitere Verwendung und die Speicherdauer der Daten bleiben ungewiss. Die Presse berichtete erst jüngst im November, die USA wollten Passagierdaten von Einreisenden 50 Jahre lang speichern. Auch der zur Verfügung gestellte Datensatz mit Daten z. B. über Sitzplatznummer, Zahlungsart, Reisebüro oder Essgewohnheiten ist weiterhin viel zu umfangreich.

Im Spätsommer berichteten seriöse Zeitungen, nachdem Innenminister Schäuble in einer Pressekonferenz ein positives Resümee über den Verlauf der Fußball-WM gezogen habe, dass der Minister mit der Begründung: „Jetzt dürfe man nicht die Hände in den Schoß legen, denn die Terrorgefahr sei während der WM weiter gewachsen“, das Antiterrordateigesetz präsentiert habe. So kam es denn auch. Auf Bundesebene standen die Beratung und Verabschiedung über das Terrorismusbekämpfungsergänzungsgesetz und das Gesetz zum Aufbau einer gemeinsamen Datei von Polizei und Nachrichtendiensten (vgl. Ziff. 9.4 dieses Berichts) an, die beide die Aufgaben und Befugnisse von Polizei und Nachrichtendiensten erweitern. Dabei wurden auch die durch das Terrorismusbekämpfungsgesetz im Jahre 2002 eingeführten Kompetenzen der Nachrichtendienste ohne Änderungen neu aufgelegt. Dabei war in das Gesetz eine Befristung aufgenommen worden, um vor einer Verlängerung die Regelungen einer gründlichen Überprüfung zu unterziehen und ungenutzte Instrumente des Rechtsstaats wieder abzuschaffen (vgl. Ziff. 9.3 und auch 9.16 dieses Berichts). Auch die ständig stark ansteigende Zahl an Telefonüberwachungsmaßnahmen spricht Bände (vgl. Grafik unter Ziff. 22.3 dieses Berichts). Seit dem 11. September 2001 hat es eine Verschärfung der Sicherheitsgesetze gegeben, die in der Geschichte der Bundesrepublik ihresgleichen sucht. Dabei ist es häufig nicht die Praxis, die nach immer neuen Eingriffsgrundlagen sucht, sondern es sind die Innenpolitiker, die bei jedem Vorfall Handlungsfähigkeit beweisen wollen. Ein Kritiker nannte dieses Phänomen jüngst ein dringendes Adoptionsbedürfnis deutscher Politiker für britische Terrorängste. In der Demokratie gibt es ein natürliches Spannungsfeld zwischen Sicherheitsbedürfnis und Freiheitsrechten. Die eine Frage ist, ob die Balance gehalten wird oder ob wir uns rapide in Richtung Überwachungsstaat bewegen. Die andere Frage ist, ob nicht durch unangemessene Maßnahmen der Kampf gegen den Terrorismus erschwert wird. Die vom Bundesverfassungsgericht für verfassungswidrig erklärte Durchführung einer Rasterfahndung ohne konkrete Gefahr (vgl. Ziff. 9.2 dieses Berichts) war solch eine Maßnahme. Sie hat in der Sache faktisch nichts erbracht, wurde aber insbesondere von Betroffenen moslemischen Glaubens als unberechtigtes Misstrauen empfunden und hat sie gegen den Staat aufgebracht. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist in einer Entschließung kritisch auf die Durchführung der Rasterfahndung eingegangen (vgl. Ziff. 19.8 dieses Berichts)

1.4 Schwerpunkte der Begleitung technischer Entwicklungen

Im privaten Bereich verfolge ich schwerpunktmäßig die Entwicklung bei der Internet-Telefonie, der RFID-Technik (vgl. Ziff. 18.2 dieses Berichts) und die Entwicklung verschiedener DV-Techniken, die in Kraftfahrzeugen zum Einsatz kommen sollen. Beispielhaft sei der in Krankenwagen bei der Feuerwehr Bremen eingesetzte UDS-Speicher erwähnt, dessen Einsatz und Funktionsweise ich bereits im letzten

Jahresbericht (vgl. 28. JB, Ziff. 6.3) dargestellt habe. Die Technik arbeitet in der Regel mit GPS und teils auch biometrischen, in jedem Falle mit fahrer- oder eignerbezogenen Daten. Die Daten sollen je nach Anwendung mit einer Dockingstation auslesbar im Fahrzeug selbst gespeichert oder an dritte Stellen via Satellit oder über Handyfrequenzen laufend oder ereignisbezogen übertragen werden. Es ist dabei nicht Aufgabe des Datenschutzes zu überprüfen, wie sinnvoll solche technischen Entwicklungen sind, sondern es ist nur darauf zu achten, wie das informationelle Selbstbestimmungsrecht gewahrt werden kann. Und Wege hierfür konnten bisher immer aufgezeigt werden. Die Datenschutzbeauftragten und die Datenschutzaufsichtsbehörden des Bundes und der Länder haben zur Begleitung dieser Entwicklung eine gemeinsame Arbeitgruppe eingesetzt, der ich angehöre. Erste Kontakte mit der Autoindustrie und den Zulieferbetrieben hat es im Berichtsjahr gegeben.

1.5 Schriftliche Eingaben und telefonische Anfragen von Bürgerinnen und Bürgern

Im Jahre 2006 erhielt ich erneut eine hohe Zahl von schriftlichen Eingaben von Bürgern, die sich an mich wegen der Verarbeitung ihrer personenbezogenen Daten durch Behörden, Unternehmen oder andere datenverarbeitende Stellen wandten. Im öffentlichen Bereich ging es bei den Eingaben am häufigsten um Fragen aus dem Bereich der inneren Sicherheit, speziell der Polizei. Fast ebenso starken Anteil hatte der Bereich Jugend, Familie und Soziales; wie bereits im Jahr zuvor bezogen sich dabei viele Fragen auf die Datenverarbeitung der BAgIS. Eine erhebliche Anzahl Eingaben betrafen auch die Datenverarbeitung im Gesundheitsbereich, hier insbesondere zur Kranken- und Pflegeversicherung.

Im nicht öffentlichen Bereich hatten Eingaben, die den Bereich Internet/Telekommunikation betrafen, den höchsten Anteil. Sehr häufig erhielt ich auch Eingaben zur Videoüberwachung durch Unternehmen und Wohnungseigentümer, zum Arbeitnehmerdatenschutz in den Betrieben und zur Datenverarbeitung der Auskunfteien.

Darüber hinaus bekam ich eine Vielzahl telefonischer Anfragen zu den verschiedenen Bereichen der Datenverarbeitung. Um die Vielfalt dieser Anfragen darzustellen, habe ich einige der Themen aus dem Berichtsjahr in einer Tabelle erfasst (vgl. Ziff. 22.2 dieses Berichts). Die dort aufgeführten Fragen wurden alle telefonisch beantwortet. Insgesamt gesehen stieg die Zahl der Eingaben und Anfragen im Berichtsjahr im Vergleich zum Vorjahr weiter an.

1.6 Zur Situation der Dienststelle

Das Berichtsjahr 2006 war für die Dienststelle mit einigen zum Teil unvorhersehbaren Turbulenzen verbunden, verursacht durch die personelle Situation. Davon war einiges vorhersehbar, anderes kam unerwartet. Vorhersehbar waren die durch Altersteilzeit bedingten Ausfälle, die u. a. zwei von sechs Referaten betreffen. Hinzu kamen weitere nicht planbare Abgänge durch Beurlaubung, Beendigung des Dienstverhältnisses und Abberufung zu einer anderen senatorischen Dienststelle. Ich hatte zwar in den Haushaltsberatungen um einen Ausgleich für die durch die Freistellung für Altersteilzeit bedingten Ausfälle gebeten, der mir aber nicht gewährt wurde. Zu diesem Zeitpunkt war aber die weitere dramatische Entwicklung noch nicht absehbar. Im Laufe des Jahres verschlechterten sich die personellen Ressourcen kontinuierlich. Seit Ende 2006 müssen zwei Referenten die anderen vier Referate mit vertreten. Ein geordnetes Arbeiten ist da natürlich nicht mehr möglich. Wenn ich nicht gleich den Notstand ausgerufen habe, dann nur deshalb, weil auch die Stürme mit orkanartigen Böen immer erst Bremerhaven heimsuchen, bevor sie abgeschwächt in Bremen einfallen. Enttäuschung über mangelnde Unterstützung zur Überbrückung des personellen Engpasses ist schon in der Dienststelle zu verspüren, aber für 2007 gibt es Anzeichen, dass die personelle Situation sich entscheidend verbessern wird. Wichtig ist, mit eingearbeitetem Personal wieder Kontinuität und Effektivität zu erreichen.

1.7 Vorträge, Fortbildungsangebot und Kooperationen

In 2006 führten die Mitarbeiterinnen und Mitarbeiter der Dienststelle wieder mehrere Fortbildungsmaßnahmen durch. Den beim Magistrat der Stadt Bremerhaven Ende 2005 neu bestellten behördlichen Datenschutzbeauftragten bot ich gleich zu Beginn des Berichtsjahres ein Fortbildungsseminar an, das ihrer Einführung in die

neue Tätigkeit diente. Außerdem wurde im Aus- und Fortbildungszentrum der bremischen Verwaltung ein Fortbildungsseminar zur „Einführung in das Datenschutzrecht“ gehalten, an dem interessierte Teilnehmer aus allen Bereichen der Verwaltung teilnahmen. Mehrere Vorträge zum Thema „Datenschutzaspekte beim Bürokommunikations- und Archivierungssystem VISkompakt“ und zu der von mir erarbeiteten „Orientierungshilfe zur Erstellung eines Datenschutzkonzeptes“ wurden von den Mitarbeiterinnen und Mitarbeitern der Dienststelle in Workshops für die behördlichen Datenschutzbeauftragten behandelt (vgl. Ziff. 2.1 dieses Berichts).

Vorträge zu den Themen „Konsequenzen aus dem Mittelstandsentlastungsgesetz für den betrieblichen Datenschutz“ und „Informationsfreiheitsgesetz“ hielt ich vor betrieblichen Datenschutzbeauftragten im Erfa-Kreis Bremen/Weser-Ems. Weiterhin kooperierte ich im Berichtsjahr mit dem Virtuellen Datenschutzbüro, dessen Federführung beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein liegt, und der datenschutz nord GmbH. Die Zusammenarbeit mit den Datenschutzbeauftragten des Bundes und der Länder sowie mit den Datenschutzaufsichtsbehörden versteht sich von selbst.

2. Behördliche Beauftragte für den Datenschutz

2.1 Workshops der behördlichen Datenschutzbeauftragten

Gemäß § 7 a Abs. 1 Bremisches Datenschutzgesetz (BremDSG) haben öffentliche Stellen einen behördlichen Datenschutzbeauftragten zu bestellen. Nachdem die überwiegende Zahl der zumeist neu bestellten behördlichen Datenschutzbeauftragten an den von mir abgehaltenen Einführungsseminaren (vgl. 28. JB, Ziff. 2.1) teilgenommen hatte, habe ich im Berichtsjahr für diesen Personenkreis Workshops zu zwei Themen durchgeführt. Mit den Workshops möchte ich die behördlichen Datenschutzbeauftragten nach den Einführungsseminaren auch weiterhin bei der Wahrnehmung ihrer Aufgaben unterstützen. Aktuelle Themen, die möglichst für alle Dienststellen der Verwaltung von Bedeutung sind und von den behördlichen Datenschutzbeauftragten auch selbst vorgeschlagen werden können, sollen vertieft erörtert werden. Außerdem sollen diese Treffen dem Erfahrungsaustausch der behördlichen Datenschutzbeauftragten untereinander dienen.

Schwerpunktthemen der Workshops waren die „Datenschutzaspekte beim Bürokommunikations- und Archivierungssystem VISkompakt“ und die von mir erarbeitete „Orientierungshilfe zur Erstellung eines Datenschutzkonzeptes“ (vgl. Ziff. 6.1 dieses Berichts). Beide Schwerpunkte stießen bei den behördlichen Datenschutzbeauftragten auf erhebliche Resonanz, so dass zu beiden Themen jeweils mehrere Veranstaltungen durchgeführt werden mussten.

Im Anschluss an das Schwerpunktthema kam es in den Veranstaltungen regelmäßig zu einer ausführlichen Diskussion, in die die behördlichen Datenschutzbeauftragten auch die bislang bei ihrer Tätigkeit gewonnenen Erfahrungen einfließen ließen. Hierbei ergab sich u. a., dass die Unterrichtung und Beteiligung der behördlichen Datenschutzbeauftragten, insbesondere im Hinblick auf die Einführung oder den Einsatz automatisierter Verfahren, mit denen personenbezogene Daten verarbeitet werden, in den Dienststellen häufig noch verbesserungsbedürftig sind. Die behördlichen Datenschutzbeauftragten können die von ihnen wahrzunehmenden Aufgaben nur erfüllen, wenn die verantwortlichen Stellen den sich für sie gegenüber ihren Datenschutzbeauftragten insbesondere aus den §§ 7, 7 a und 8 BremDSG ergebenden Verpflichtungen nachkommen. Nachlässigkeiten können in Übergangszeiten entstehen, die genannten Regelungen sind aber mittlerweile so lange in Kraft, dass in Zukunft Versäumnisse nicht mehr hingenommen werden können.

3. Bremisches Datenschutzaudit

3.1 Datenschutzaudit – Zulassung eines Auditors

Öffentliche Stellen können nach § 7 Bremisches Datenschutzgesetz (BremDSG) zur Verbesserung des Datenschutzes und der Datensicherheit ihre Verfahren sowie ihre technischen Einrichtungen durch unabhängige Gutachter prüfen und bewerten lassen (Auditierung). Ziel des Datenschutzaudits ist die Verbesserung des Datenschutzes und der Datensicherheit. Durch das Audit soll die Selbstverantwortung der Datenverarbeiter gefördert werden. Näheres zu Inhalt und Ausgestaltung des Prü-

fungs- und Bewertungsverfahrens hat der Senat durch die Bremische Datenschutzauditverordnung vom 5. Oktober 2004 geregelt (Brem.GBl. 2004, S. 515). Nach der Verordnung sind öffentliche Stellen auch berechtigt, für erfolgreich auditierte Verfahren für einen Zeitraum von zwei Jahren das Bremische Datenschutzaudit-Gütesiegel zu verwenden.

Die Prüfung und Bewertung eines DV-Verfahrens wird durch einen Auditor vorgenommen, der auf Vorschlag der öffentlichen Stelle zur Wahrnehmung dieser Aufgabe vom Landesbeauftragten für Datenschutz und Informationsfreiheit zugelassen werden kann. Zugelassen wird grundsätzlich nur, wer seine fachliche Eignung, persönliche Zuverlässigkeit und Unabhängigkeit für die Tätigkeit als Auditor nachweist. Nähere Regelungen zur Zulassung, insbesondere zu den von den Auditoren zu erfüllenden Anforderungen, enthalten die Durchführungsbestimmungen zur Bremischen Datenschutzauditverordnung. Die genannten Rechtsquellen sind im Internet unter www.datenschutz.bremen.de/audit abrufbar.

Im Berichtsjahr erteilte ich erstmals einem Bewerber für die Auditierung eines DV-Verfahrens die Zulassung. Ein Entsorgungsunternehmen hatte mir zuvor mitgeteilt, dass es ein Verfahren für die Wahrnehmung ihm übertragener öffentlicher Aufgaben prüfen und bewerten lassen möchte und hat hierfür einen Auditor vorgeschlagen. Ich prüfte, ob der vorgeschlagene Bewerber die Anforderungen nach der Bremischen Datenschutzauditverordnung, bezogen auf das zur Prüfung und Bewertung vorgesehene Verfahren, erfüllt. Dies war vom Bewerber entsprechend nachzuweisen. Ich erteilte daraufhin in einem Bescheid die Zulassung.

4. Internet, Telekommunikation, Teledienst

4.1 Terrabyte von Telefondaten sollen auf Vorrat gespeichert werden

Im letzten Jahresbericht hatte ich über die Verabschiedung der Richtlinie zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten (RL 2006/24/EG) und meine datenschutzrechtlichen und verfassungsrechtlichen Bedenken berichtet (vgl. 28. JB, Ziff. 3.2). Die Richtlinie ist am 3. Mai 2006 in Kraft getreten. Noch im Mai 2006 haben die Länder Irland und Slowakei Klage vor dem Europäischen Gerichtshof in Luxemburg gegen die Richtlinie erhoben. Sie sind der Auffassung, dass die Regelung nur in einem so genannten Rahmenbeschluss, nicht aber in einer Richtlinie hätte getroffen werden können. Eine Entscheidung des Europäischen Gerichtshofs steht noch aus und wird wohl erst nach Ablauf der Umsetzungsfrist in nationales Recht am 15. September 2007 ergehen. Auch nach einem Gutachten des wissenschaftlichen Dienstes des Deutschen Bundestages bestehen erhebliche Bedenken, ob die Richtlinie mit dem Europarecht und den dort verankerten Grundrechten vereinbar ist.

Das Bundesministerium der Justiz hat Ende November 2006 einen Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vorgelegt. Die Speicherungspflicht für Verkehrsdaten, die den Telekommunikationsunternehmen ohne Kostenerstattung auferlegt wird, wird durch die neuen §§ 110 a und 110 b Telekommunikationsgesetz (E-TKG) geregelt.

Nach § 110 a E-TKG soll eine Speicherung nur für die von der Richtlinie vorgegebene Mindestdauer von sechs Monaten erfolgen. Gespeichert werden sollen die Rufnummern des Anrufers und Angerufenen, Beginn und Ende der Verbindung, der genutzte Dienst, sowie zusätzlich bei Mobilfunkgeräten die Kennungen der Mobilfunkkarten bzw. des anrufenden oder angerufenen Endgeräts und die Funkzelle, bei Internettelefonie zusätzlich die Internetprotokoll-Adressen. Bei elektronischer Internetkommunikation (Web, E-Mail) sollen die Adresse von Empfänger und Absender, die Internetprotokoll-Adressen und Beginn und Ende der Nutzung des Dienstes gespeichert werden, bei Internetzugangsdiensten eine eindeutige Kennung des Anschlusses, über den die Internetnutzung läuft, Beginn und Ende der Internetnutzung und die zugewiesene Internetprotokoll-Adresse. Zu speichern sind auch Anrufversuche. Daten, die Aufschluss über den Inhalt der Kommunikation geben, dürfen nicht gespeichert werden.

Die Verwendung der gespeicherten Daten beschränkt § 110 b Abs. 1 Satz 1 E-TKG derzeit auf die Verfolgung von Straftaten. Eine Ausweitung auf Zwecke der Gefahrenabwehr oder andere Zwecke im Laufe des Gesetzgebungsverfahrens ist damit

nicht ausgeschlossen. Obwohl weiterhin grundsätzlich verfassungsrechtliche Bedenken bestehen, werde ich mich im Arbeitskreis Justiz der Landesbeauftragten für den Datenschutz des Bundes und der Länder mit dem Referentenentwurf näher auseinandersetzen.

4.2 Urteil des Bundesverfassungsgerichts zum IMSI-Catcher

Mit Beschluss vom 22. August 2006 (2 BvR 1345/03) hat das Bundesverfassungsgericht die Ermittlung der Gerätenummer eines Mobilfunkgeräts (IMEI: International Mobile Equipment Identity) und Kartennummer einer SIM-Karte (IMSI: International Mobile Subscriber Identity) sowie des Standorts von Mobiltelefonen durch den so genannten IMSI-Catcher nach § 100 i StPO für verfassungsgemäß erklärt.

Grundlage des IMSI-Catcher ist, dass jedes Mobiltelefon wie auch jede SIM-Karte mit einer weltweit nur einmal vergebenen Nummer versehen ist, über die der Mobilfunkteilnehmer ermittelt werden kann. Voraussetzung für den Einsatz der technischen Anlage eines so genannten IMSI-Catcher ist die ungefähre Kenntnis des Standorts des gesuchten Mobiltelefons. Der IMSI-Catcher macht sich zunutze, dass sich alle Mobiltelefone im empfangsbereiten Zustand in kurzen Abständen bei der für sie gerade „zuständigen" Basisstation des Mobilfunknetzes anmelden. Das gesamte Mobilfunknetz ist entsprechend einem Raster in einzelne Zellen aufgeteilt. Im Rahmen dieser ständigen Positionsangabe werden unter anderem die IMSI und die IMEI an die Basisstation gesendet. Die Erfassung der IMSI und IMEI erfolgt dadurch, dass innerhalb einer solchen Funkzelle der IMSI-Catcher die Basisstation des Mobilfunknetzes simuliert. Sämtliche eingeschalteten Mobiltelefone, die sich im Einzugsbereich des IMSI-Catcher befinden, senden nunmehr ihre Daten an diesen. Durch eine verstärkte Sendeleistung des IMSI-Catcher ist diese simulierte Funkzelle erheblich kleiner als die reguläre Funkzelle. Befinden sich in der simulierten Funkzelle mehrere Mobilfunkteilnehmer, sind zur Bestimmung des gesuchten Mobiltelefons mehrere Messungen erforderlich. Dabei werden an verschiedenen Orten Messungen durchgeführt und nach einem statistischen Auswerteprinzip in Form von Schnittmengen die jeweiligen IMSI/IMEI ermittelt oder zumindest eingegrenzt. Auf diese Weise lässt sich der Standort des gesuchten Gerätes sehr genau ermitteln.

Das Bundesverfassungsgericht hat festgehalten, dass die Erhebung dieser Daten nicht unter den Schutz des Fernmeldegeheimnisses (Art. 10 GG) fällt. Die Feststellung einer Geräte- oder Kartennummer eines im Bereich einer simulierten Funkzelle befindlichen Mobiltelefons durch den Einsatz eines IMSI-Catcher ist unabhängig von einem tatsächlich stattfindenden oder zumindest versuchten Kommunikationsvorgang zwischen Menschen. Es fehlt an einem menschlich veranlassten Informationsaustausch, der sich auf Kommunikationsinhalte bezieht. Es „kommunizieren" ausschließlich technische Geräte miteinander. Die bloße technische Eignung eines Mobilfunkgeräts, als Kommunikationsmittel zu dienen sowie die von dem Gerät ausgehenden technischen Signale zur Gewährleistung der Kommunikationsbereitschaft stellen noch keine Kommunikation dar. Das Bundesverfassungsgericht prüfte und bejahte zwar auch einen Eingriff in das Recht auf informationelle Selbstbestimmung, sah diesen Eingriff jedoch durch die gesetzliche Regelung in § 100 i StPO als gerechtfertigt an und verneinte insbesondere einen unverhältnismäßigen Eingriff.

4.3 Urteil des Bundesverfassungsgerichts zur Handy- und PC Überwachung

Das Bundesverfassungsgericht hat mit Urteil vom 2. März 2006 (2 BvR 2099/04) das Recht auf informationelle Selbstbestimmung gestärkt. Dem Verfahren lag die Verfassungsbeschwerde einer Richterin zugrunde, deren Wohnung wegen des Verdachts der Verletzung von Dienstgeheimnissen durchsucht worden war. Dabei war u. a. auf die auf ihrem Computer gespeicherten Daten sowie den Einzelverbindungsnachweis ihres Mobilfunktelefons zugegriffen worden. Die Durchsuchung erbrachte keine strafrechtlich verwertbaren Anhaltspunkte.

Das Verfassungsgericht hielt fest, dass die im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Telekommunikationsverbindungsdaten nach Abschluss des Übertragungsvorgangs nicht mehr durch das Fernmeldegeheimnis (Art. 10 Abs. 1 GG) geschützt sind. Denn anders als bei dem Kommunikationsprozess, bei dem der Teilnehmer keinen Einfluss auf die Entstehung oder Speicherung der Verbindungsdaten durch Nachrichtenermittler besitzt, kann der Teilnehmer

nach Abschluss des Vorgangs den Zugriff auf die sich in seiner Sphäre befindlichen Daten durch vielfältige technische Vorkehrungen verhindern.

Die in der Herrschaftssphäre des Teilnehmers gespeicherten personenbezogenen Verbindungsdaten unterliegen jedoch dem Schutz durch das Recht auf informationelle Selbstbestimmung (Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG) und gegebenenfalls durch das Recht auf Unverletzlichkeit der Wohnung (Artikel 13 Abs. 1 GG). Ein Eingriff bedarf danach jeweils im konkreten Fall einer Rechtfertigung nach dem Grundsatz der Verhältnismäßigkeit. Die Verhältnismäßigkeitsprüfung muss dem Umstand Rechnung tragen, dass es sich um Daten handelt, die außerhalb der Sphäre des Betroffenen unter dem besonderen Schutz des Fernmeldegeheimnisses stehen und denen im Herrschaftsbereich des Betroffenen ein ergänzender Schutz durch das Recht auf informationelle Selbstbestimmung zuteil wird. Der Maßnahme können im Einzelfall daher die Geringfügigkeit der zu ermittelnden Straftat, eine geringe Beweisbedeutung sowie die Unbestimmtheit des Auffindungsverdachts entgegenstehen. Die Durchsuchungsanordnung muss zudem auf den tatsächlich erforderlichen Umfang begrenzt werden, etwa durch eine zeitliche Eingrenzung oder die Beschränkung auf bestimmte Kommunikationsmittel.

5. Medien

5.1 Verfahren der Rundfunkgebührenbefreiung

Im vergangenen Jahr hatte ich über das Verfahren zur Rundfunkgebührenbefreiung berichtet (vgl. 28. JB, Ziff. 5.1). § 6 Abs. 2 des 8. Rundfunkgebührenstaatsvertrages sieht vor, dass für die Befreiung die Vorlage des Bewilligungsbescheids im Original oder in beglaubigter Kopie erforderlich ist. Da sich in den Bewilligungsbescheiden von Arbeitslosengeld, Sozialhilfe oder BAföG eine Vielzahl sensibler besonders schutzwürdiger Daten befinden, die für eine Rundfunkgebührenbefreiung nicht erforderlich sind, bedeutete deren Vorlage einen gravierenden Eingriff in das Recht auf informationelle Selbstbestimmung.

Es hatte hier verschiedene Versuche gegeben, eine datenschutzkonforme Lösung herbeizuführen, indem etwa der Befreiungsantrag mit dem Hinweis abgestempelt wird, der Originalbescheid habe vorgelegen. Dieses Verfahren wurde wiederum von der GEZ nicht anerkannt. In mehreren Treffen eines so genannten Runden Tisches in Bremen wurde versucht, das Verfahren zu vereinfachen. Auch der Rechtsausschuss und die Bremische Bürgerschaft haben sich mit diesen Themen beschäftigt (vgl. Antrag Drs. 16/1141) und Debatte vom 16. November 2006 (vgl. Plenarprotokoll der Bürgerschaft/Landtag S. 4751 ff.).

Im Ergebnis wird nun von der GEZ eine so genannte Drittbescheinigung akzeptiert, die nur die für die Rundfunkgebührenbefreiung erforderlichen Daten enthält und von den Betroffenen zusammen mit dem Befreiungsantrag abgegeben und von der Bewilligungsbehörde ausgefüllt und bestätigt wird. Eine grundlegende Änderung des Verfahrens kann nur durch eine Änderung des Rundfunkgebührenstaatsvertrages herbeigeführt werden.

6. Datenschutz durch Technikgestaltung und -bewertung

6.1 Orientierungshilfe zur Erstellung eines Datenschutzkonzeptes

Häufiges Diskussionsthema bei Schulungen und Workshops für behördliche Datenschutzbeauftragte war in der Vergangenheit die Erstellung der Verfahrensbeschreibungen bei der verantwortlichen Stelle, und hier insbesondere die Darstellung der technischen und organisatorischen Maßnahmen nach § 7 Bremisches Datenschutzgesetz (BremDSG).

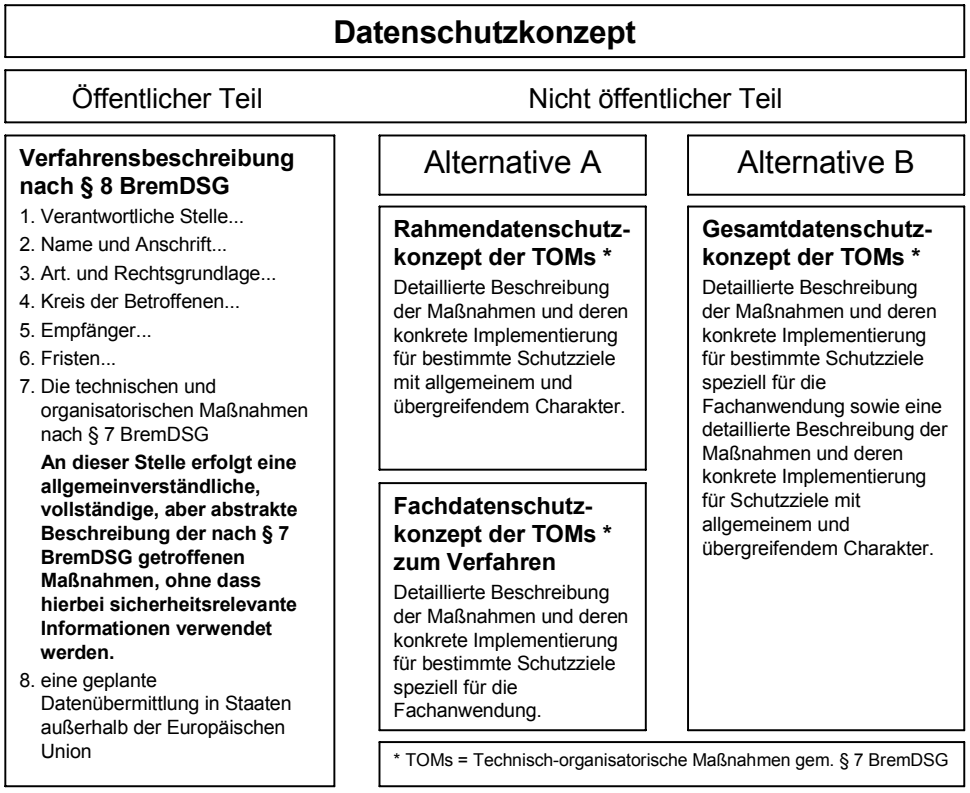
Ich habe daher im Berichtsjahr eine Orientierungshilfe erarbeitet, die den behördlichen Datenschutzbeauftragten als Hilfestellung bei dieser Aufgabe dienen soll. Dabei wurde es notwendig, eine klare Linie zu ziehen zwischen den für jedermann öffentlich zugänglichen Verfahrensbeschreibungen und den in einem Konzept festzulegenden Sicherheitsvorkehrungen, die natürlich nicht öffentlich gemacht werden sollen.

Nach § 8 BremDSG ist eine Verfahrensbeschreibung zu erstellen, die öffentlich einsehbar ist. Anders als im Bundesdatenschutzgesetz sind die technischen und orga-

nisatorischen Maßnahmen davon nicht ausgenommen. Von Administratoren wurde dieser Sachverhalt kritisiert, denn es bestehe die Gefahr, dass bei der Beschreibung der getroffenen Maßnahmen sicherheitsrelevante Informationen dargestellt werden, die nicht für eine öffentliche Einsichtnahme geeignet seien. Eine detaillierte Beschreibung der Sicherheitsinfrastruktur ist aber in der Regel erforderlich, um eine datenschutztechnische Bewertung durchführen zu können.

Um diesem Dilemma zu entgehen, habe ich folgende Vorgehensweise empfohlen: Die Verfahrensbeschreibung soll bezüglich der technischen und organisatorischen Maßnahmen eine Beschreibung auf abstraktem Niveau enthalten, die bei Einsichtnahme durch den Bürger verstanden werden kann. Ergänzt werden soll diese Verfahrensbeschreibung dann um ein nicht öffentliches Fachdatenschutzkonzept, welches die Maßnahmen zur Erreichung der Schutzziele detailliert beschreibt und eine Bewertung der getroffenen Maßnahmen ermöglicht. Sollen mehrere oder integrierte Verfahren beschrieben werden, können solche Maßnahmen, die für alle Verfahren gelten (z. B. Zutrittskontrolle zu Serverräumen, Zugangskontrolle bezüglich Anmeldeverfahren am PC-Arbeitsplatz, zentrale Datensicherungskonzepte) in einem Rahmendatenschutzkonzept zusammengefasst werden.

Das skizzierte Konzept wird derzeit den behördlichen Datenschutzbeauftragten mitgeteilt und bereits in ersten größeren Behörden, z. B. beim Stadtamt Bremen, umgesetzt.



6.2 Protokollierung und Revision

Im Berichtsjahr habe ich bei meinen Prüfungen und Beratungen festgestellt, dass eine sachgerechte Protokollierung und Revision in komplexen DV-Systemen mit Anforderungen verbunden ist, die umfangreiche konzeptionelle Überlegungen erfordert. Die Protokollierung und darauf aufsetzend die Revision sind zu eigenen Verfahren geworden. Sie fallen insbesondere bei vielschichtigen Verarbeitungsprozessen nicht mehr „nebenbei“ in Form einer speziellen, bestenfalls noch überschaubaren Logdatei an, sondern sind viel umfangreicher und erfordern eine gezielte Planung. Angesichts des rasanten Aufbaus neuer Systeme wird für eine datenschutzgerechte Konzeption der Protokollierung oft nicht die nötige Zeit eingeplant.

Unter Protokollierung beim Betrieb von IT-Systemen im datenschutzrechtlichen Sinn wird die Erstellung von manuellen, in der Regel automatisierten Aufzeichnungen verstanden, aus denen insbesondere nachvollziehbar sein muss, welche Person zu einem bestimmten Zeitpunkt mit welchen Funktionen auf personenbezogene Daten zugegriffen hat. Hinzu kommt, dass Systemzustände, wie beispielsweise die Do-

kumentation der Zugriffssystematik über einen definierten Zeitraum, ableitbar sein müssen.

Die rechtlichen Verpflichtungen ergeben sich dabei direkt aus den Datenschutzgesetzen. Das Bundesdatenschutzgesetz (BDSG) schreibt in der Anlage zu § 9 Nr. 4 und 5 und das Bremische Datenschutzgesetz (BremDSG) in § 7 Abs. 4 Satz 2 Nr. 4 und 5 entsprechende Dokumentationen in Rahmen der Eingabe- und Weitergabekontrolle vor. Auch im Zusammenhang mit automatisierten Abrufverfahren sind solche Protokolle zu erstellen (§ 14 Abs. 3 BremDSG). Im Security Management muss durch Zugangskontrolle und Rechteverwaltung dafür gesorgt werden, dass nur Berechtigte in der Lage sind, auf Protokolle zuzugreifen. Hierzu gehört beispielsweise als technische Maßnahme die Speicherung der Daten außerhalb der produktiven Systeme, auch um die Anforderung der Revisionsfähigkeit umzusetzen.

Diese Protokolldaten unterliegen selbst wieder eigenen Datenschutzregelungen. So dürfen die in diesem Rahmen erhobenen personenbezogenen Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, nur für diese Zwecke verwendet werden (besondere Zweckbindung). Es ist also das Verfahren der Protokollierung selbst und damit verbunden der Schutz der in diesem Rahmen erhobenen personenbezogenen Daten technisch und organisatorisch zu klären. Da im Rahmen der Protokollierung Daten von Arbeitnehmern und Arbeitnehmerinnen verarbeitet werden, ist das Verbot der Leistungs- und Verhaltenskontrolle (vgl. § 20 BremDSG) zu garantieren. Eine weitere datenschutzrechtliche Anforderung gilt natürlich grundsätzlich auch hier: Das Prinzip der Datensparsamkeit und Datenvermeidung (§ 7 BremDSG, § 3 a BDSG).

Vor diesem Hintergrund muss die Protokollierung hinsichtlich ihrer Art, ihrer Ziele, ihrer Inhalte und Auswertbarkeit beschrieben werden. Es gibt Protokolle auf verschiedenen Systemebenen, die sich auf benutzer-, prozess- oder/und sicherheitstechnische Ereignisse beziehen. Diese Protokolle dienen grundsätzlich zwei Zielen: Es soll möglich sein, Sicherheitsverletzungen durch Aufzeichnung sicherheitsrelevanter Ereignisse zu erkennen. Außerdem müssen für Zwecke der Beweissicherung Handlungen von Benutzern im System nachvollziehbar sein. Mit einer revisionssicheren Protokollierung der Systemadministration kann beispielsweise die Frage beantwortet werden, welcher Administrator zu welchem Zeitpunkt welche das Security Management betreffenden Aktionen (wie etwa Änderung einer Sicherheitsregel, Ändern von Benutzerrechten, Löschen von Logdateien) durchgeführt hat. Auch die Durchführung von Servicearbeiten muss entsprechend nachvollziehbar sein. Die Protokollierung von Administratortätigkeiten dient der Kontrolle der gesamten Systemsicherheit. Sie kann auch Schutz vor eventuellen Verdächtigungen bieten.

In der Praxis habe ich häufig die Erfahrung gemacht, dass die Administratoren die Revisionsmöglichkeit ihrer Tätigkeit ablehnen. Sie argumentieren, dass eine Vertrauensposition, die uneingeschränkte Aktivitäten in den Systemen ermöglicht, nicht umfassend kontrolliert werden kann und dies auch nicht erforderlich sei. Es gibt jedoch in komplexen DV-Systemen eine Vielzahl administrativer Tätigkeiten, die von verschiedenen Personen und auch externen Firmen wahrgenommen werden. In diesem Umfeld existiert die klassische, an eine Person gebundene Vertrauensposition nicht mehr. Hinzu kommt, dass der Verarbeitungsumfang bezogen auf Datenmengen und Möglichkeiten (insbesondere Verknüpfungen von Informationen und Datenabgleiche) stark zugenommen hat. Es ist daher wichtig, die Aufzeichnungen nach bestimmten Fragestellungen auswertbar zu machen. Hierfür sind entsprechende Tools einzusetzen, um ein „Ereignismanagement“ zu ermöglichen.

Aufgrund der im Rahmen einer sinnvollen Protokollierung und Revision zu behandelnden Fragestellungen wird deutlich, dass eine Grundlage für die konzeptionelle Gestaltung dieses Verfahrens bereits im Rahmen einer Sicherheitspolicy, die u. a. Basisdefinitionen für die Sicherheit allgemein vornimmt, geschaffen werden muss. In diesem Rahmen müssen grundlegende Überprüfungsmodalitäten festgelegt werden.

Ich halte zur Erfüllung der datenschutzrechtlichen Normen eine sachgerechte, nicht ausufernde Protokollierung für unbedingt notwendig. Der Aufwand für die Gestaltung der Verfahren zur Protokollierung und zur Revision, verbunden mit der Konzeption des Sicherheitsmanagements bei der Einführung und Administration von

Verfahren, darf im Hinblick auf die hierfür erforderlichen Ressourcen weder aus den Augen verloren noch unterschätzt werden.

6.3 Funktionstrennung: Berechtigungen entsprechend der Aufgaben vergeben

Die Zahl der Informationssysteme wächst stetig und schnell. Und mit ihnen die Zahl der darin gespeicherten und verarbeiteten Daten. Mit der Anzahl der Informationssysteme wächst aber auch die Aufgabenflut für die Administratoren, die (oft) mehrere davon gleichzeitig betreuen müssen. Auch in der öffentlichen Verwaltung in Bremen ist diese Entwicklung deutlich bemerkbar.

Die große Zahl der verschiedenen Systeme bedingen aber auch eine genaue Planung und Umsetzung von differenzierten Berechtigungskonzepten für die jeweils im Einsatz befindlichen Systeme. Berechtigungen regeln, wer in IT-Systemen welche Funktionen nutzen darf. Grundsätzlich ist bei diesen Berechtigungen von zwei verschiedenen Ebenen auszugehen: Den Berechtigungen, die unbedingt dazu notwendig sind, das System zu betreiben (administrative Berechtigungen) und die Berechtigungen, die zur Aufgabenerfüllung notwendig sind (operative Berechtigungen).

Aus Sicht des Datenschutzes ist eine klare Trennung zwischen diesen Bereichen anzustreben. Darüber hinaus gibt es Funktionen, die in einer Person liegend unvereinbar sind, hier muss es zwingend zu einer klaren personellen Trennung kommen (z. B. Administrator und Revisor).

Während sich die Anforderungen der personellen Trennung von Aufgaben in größeren Organisationseinheiten relativ problemlos umsetzen lassen, bestehen hierfür in kleinen Einheiten weitaus mehr Schwierigkeiten. Solange keine miteinander unvereinbaren Aufgaben betroffen sind, sind bei einer Doppelfunktion der Aufgabenwahrnehmung auf verschiedenen Ebenen besondere Regeln zu beachten. In IT-Systemen soll jeder nur mit so viel Rechten ausgestattet sein wie es zur Wahrnehmung der spezifischen Aufgaben notwendig ist. In der Literatur wird oft vom „Need-to-know-Prinzip“ gesprochen. So soll ein Administrator sich an den IT-Systemen nur dann mit administrativen Berechtigungen anmelden, wenn er auch administrative Tätigkeiten durchzuführen hat („Wartung ohne inhaltlichen Zugriff“). Bei operativer Tätigkeit muss er über den hierfür vorgesehenen Berechtigungspfad gehen. Eine Funktionstrennung wird dabei durch die Nutzung unterschiedlicher Benutzerkennungen und Passwörter erreicht.

Auch innerhalb von DV-Fachverfahren soll eine strikte Funktionstrennung umgesetzt werden. Es ist nicht auszuschließen, dass Anwender des Systems auch Aufgaben mit administrativem Hintergrund zu erledigen haben. Diese Berechtigungen sind im System getrennt voneinander abzubilden und die Funktionstrennung dadurch zu realisieren, dass wiederum je nach Aufgabe eine spezifische Anmeldung an das Fachverfahren erfolgen muss.

Strikte Funktionstrennung ist ein wichtiges Werkzeug, um ein hohes Sicherheitsniveau zu erreichen. Auch Vertretungsregelungen sollten unter Wahrung strikter Funktionstrennungen realisiert werden, womit auch Risiken minimiert und das Wissen bzw. bestimmte Fähigkeiten auf mehrere Personen verteilt werden. Letztendlich lässt sich nur durch saubere Funktionstrennung, eine Trennung zwischen Entscheidung, Ausführung, Kontrolle (und Berichterstattung), eine richtige und aussagekräftige Revision der IT-Systeme realisieren.

Zum Aufbau einer Funktionstrennung gehört, dass ein umfassendes Berechtigungskonzept erarbeitet wird, das alle notwendigen Rollen vollständig mit den zugehörigen Rechten beschreibt. Dies gilt sowohl für die in den Organisationseinheiten im Einsatz befindliche IT-Basisinfrastruktur als auch für die angewendeten Fachverfahren. Das Berechtigungskonzept ist auf aktuellem Stand zu halten, veränderten Rahmenbedingungen anzupassen und die richtigen Abbildungen sind in den Systemen turnusmäßig zu überprüfen.

6.4 Active Directory für das bremische Verwaltungsnetz

Im Berichtsjahr habe ich vom Senator für Finanzen verschiedene Unterlagen zum geplanten Echtbetrieb des bremischen Verzeichnisdienstes „Active Directory“ (AD) mit der Bitte um Stellungnahme erhalten. Ein AD ist bereits im Pilotbetrieb und wird für diverse (Test-)Anwendungen genutzt. Dieser Pilot soll in den Echtbetrieb überführt werden. Ich habe zunächst zur gesamten Infrastruktur Stellung genommen

und Basisanforderungen an den datenschutzkonformen Betrieb eines AD formuliert. Auf Grund der Vielzahl der sicherheitsrelevanten Einstellungsmöglichkeiten eines AD konnte ich mich nicht zu allen Einstellungen äußern.

Für das Bremer Verwaltungsnetz (BVN) bedeutet die Einführung des zentralen Active Directory einen tiefgreifenden Wandel; die bisherige Struktur des BVN wird komplett umgebrochen. Die herkömmliche Version des BVN ist so aufgebaut, dass die bremische Verwaltung einer geschlossenen Benutzergruppe mit gleichwertigen Partnern entspricht. Jede Dienststelle hat die alleinige tatsächliche Verfügungsgewalt über ihre DV-Systeme und die darin gespeicherten und verarbeiteten Daten. Sie verfügt allein über die Administrationsrechte für DV-Systeme und -Verfahren. Die Dienststelle kann entscheiden, wer notwendigerweise Zugriff von außen auf Systeme oder Verfahren haben muss bzw. darf, z. B. im Rahmen von Fernwartung oder Auftragsdatenverarbeitung. Diese sind vertraglich oder über eine Verwaltungsvereinbarung rechtlich geregelt. Die Dienststelle als verantwortliche Stelle nach § 2 Abs. 3 Nr. 1 des Bremischen Datenschutzgesetzes (BremDSG) hat somit die volle Kontrolle über ihre Daten und Systeme; die Anforderungen nach § 7 Abs. 3 und Abs. 4 BremDSG können unproblematisch erfüllt werden.

Mit der Einführung eines verwaltungsweiten AD geht dieser Zustand der administrativen Hoheit der jeweiligen verantwortlichen Stelle jedoch verloren. Die einzelnen Dienststellen werden als Organisationseinheiten (OU) unterhalb von Domänen oder sogar als Sub-OU unterhalb anderer OU im AD abgebildet, z. B. Dienststelle unterhalb der senatorischen Behörde. Das hat zur Folge, dass sich z. B. Administratoren hierarchisch höher liegender Ebenen grundsätzlich jederzeit Rechte verschaffen können, um auf die Systeme und die darin gespeicherten Daten der darunter liegenden Ebene zuzugreifen. Dies kann technisch nicht verhindert werden. Besonders problematisch ist dieser Umstand in sensiblen Bereichen, in denen z. B. auch Daten von Berufsgeheimnisträgern oder sonstigen Personen, die einer besonderen Schweigepflicht unterliegen, verarbeitet werden (Gesundheitsämter, Beratungsstellen etc.).

Die Architektur des AD ist mit einem grundsätzlichen Fehler behaftet: Die verantwortlichen Stellen können nicht mehr, wie in § 7 Abs. 3 und 4 BremDSG gefordert, selbst die vollständige Kontrolle über ihre Daten und Systeme ausüben. Zwar kann die lokale Administration der verantwortlichen Stelle Maßnahmen zur Abschottung gegenüber zentralen Zugriffs- und Steuerungsmöglichkeiten für eigene Ressourcen ergreifen, diese sind jedoch jederzeit durch die zentrale Administration aufhebbar. Da sich kein zentraler Durchgriff auf die Ressourcen einzelner Organisationseinheiten verhindern lässt, muss daher insbesondere auf der Ebene der lokalen und zentralen Administration eine sichere Protokollierung und Revision gegenüberstehen.

Eine leistungsfähige Revision, wie unter Ziffer 6.2 dieses Berichts beschrieben, ist in den mir vorliegenden Dokumenten des Finanzressorts zum Einsatz des AD noch nicht dokumentiert worden. Sie ist aber parallel zur Einführung des AD zur Verfügung zu stellen und alle durch die Administration ausgelösten sicherheitsrelevanten Ereignisse sind revisionssicher zu protokollieren.

Die Protokollauswertung und Revision muss durch eine vom verantwortlichen Betreiber unabhängige Instanz durchgeführt werden. Die erforderlichen Details dafür, wie etwa der physikalische Ort der Speicherung, der Inhalt der Prüfrichtlinien, Revisionshäufigkeit, Zieldefinitionen, Rechtekontrollen, Erkennen von Manipulationsversuchen, Revisionsrollen, Kontrolle der Richtlinien für die Protokollauswertung selbst etc., müssen in einem gesonderten Revisionskonzept beschrieben werden. Darüber hinaus sollte den Administratoren der Dienststellen, die zukünftig ihre Organisationseinheit innerhalb des AD zu verwalten haben, eine Guideline zur datenschutzgerechten Konfiguration ihrer Infrastruktur und Systeme innerhalb des AD zur Verfügung gestellt werden.

Für den Einsatz eines zentralen AD muss die Summe aus Revision und Protokollierung in allen Bereich des BVN und der teilnehmenden Dienststellen einen für alle transparenten und nachvollziehbaren dokumentierten Betrieb ermöglichen. Zentrale Eingriffe können dadurch zwar nicht ausgeschlossen, aber nachträglich erkannt werden. Nur so kann von der „verantwortlichen Stelle“, wie es von den Datenschutzgesetzen verlangt wird, auch tatsächlich noch Verantwortung übernommen werden.

Über die Ausgestaltung der einzelnen Anforderungen befinde ich mich mit der für die Einführung einer AD im BVN betreuenden Einheit beim Senator für Finanzen noch im Dialog.

7. Bremische Bürgerschaft – Die Arbeit des Rechtsausschusses

7.1 Ergebnisse der Beratung des 28. Jahresberichts

Bericht und Antrag des Rechtsausschusses zum 28. Jahresbericht des Landesbeauftragten für den Datenschutz vom 31. März 2006 (Drucksache 16/980) und zur Stellungnahme des Senats vom 22. August 2006 (Drucksache 16/1111)

Bericht

Die Bürgerschaft (Landtag) überwies in ihrer Sitzung am 11. Mai 2006 den 28. Jahresbericht des Landesbeauftragten für den Datenschutz vom 31. März 2006 (Drucksache 16/980) und in ihrer Sitzung am 13. September 2006 die dazu erfolgte Stellungnahme des Senats vom 22. August 2006 (Drucksache 16/1111) an den Rechtsausschuss zur Beratung und Berichterstattung.

Der Ausschuss nahm seine Beratungen in seiner Sitzung am 4. Oktober 2006 auf und stellte bei den nachfolgend aufgeführten Punkten Beratungs- und Handlungsbedarf fest:

1. Ergebnisse der Beratungen des 27. Jahresberichts (Ziffer 7.1, Ziffer 9.15),
2. ISAWeb (Ziffer 9.7),
3. Eröffnung des elektronischen Rechtsverkehrs (Ziffer 10.1),
4. Neues zur elektronischen Gesundheitskarte (Ziffer 11.2),
5. Mammographie-Screening (Ziffer 11.3),
6. Novellierung des Bremischen Schuldatenschutzgesetzes (Ziffer 13.3),
7. Prüfung des Schuldatenverwaltungsverfahrens MAGELLAN (Ziffer 13.4).

Der Rechtsausschuss erörterte die genannten Komplexe mit dem Landesbeauftragten für den Datenschutz unter Hinzuziehung der Vertreter der betroffenen Ressorts und Institutionen in seinen Sitzungen am 1. November 2006, 6. Dezember 2006 sowie am 14. Februar 2007.

Zu den einzelnen Punkten nimmt der Rechtsausschuss wie folgt Stellung:

Ergebnisse der Beratungen des 27. Jahresberichts

a) Telekommunikationsüberwachung (Ziffer 7.1): Im Rahmen der Beratungen zum 27. Jahresbericht wurde vom Senator für Inneres und Sport zugesagt, das erforderliche Datenschutzkonzept für die Komponenten des Systems der Telekommunikationsüberwachung bis Ende Februar 2006 vorzulegen. Nach Auskunft des Senators für Inneres und Sport sind aufgrund personeller Engpässe bei der Polizei Verzögerungen in der Bearbeitung aufgetreten. Der Senator für Inneres und Sport hat nunmehr den Entwurf der Verfahrensbeschreibung zur Telekommunikationsüberwachung mit Schreiben vom 10. November 2006 dem Landesbeauftragten für den Datenschutz zur weiteren Abstimmung übersandt.

Der Ausschuss nimmt zur Kenntnis, dass der Landesbeauftragte für den Datenschutz den Entwurf prüfen und den Ausschuss über das Ergebnis unterrichten wird.

b) Zentrales Datenschutzkonzept und Verfahrensbeschreibungen beim Stadtamt Bremen (Ziffer 9.15): Der Rechtsausschuss hat sich im Jahr 2006 mehrfach mit den seit mehreren Jahren beim Stadtamt Bremen zu verschiedenen DV-Verfahren ausstehenden Fachdatenschutzkonzepten und dem fehlenden Rahmendatenschutzkonzept beschäftigt. Bis zur Sommerpause hat das Stadtamt Bremen die angekündigten Fachdatenschutzkonzepte zu den Verfahren „Waffenverwaltung, Gewerbe, Meldewesen und Kfz-Zulassung“ vorgelegt. Das Rahmendatenschutzkonzept konnte aufgrund der Streikphase im Stadtamt Bremen erst zum Jahresende 2006 fertig gestellt werden und wurde dem Landesbeauftragten für den Datenschutz mit E-Mail vom 5. Januar 2007 zur Stellungnahme übersandt. Der Ausschuss nimmt den Bearbeitungsstand zur Kenntnis.

ISAWeb (Ziffer 9.7): Zu der vom Landesbeauftragten für den Datenschutz angemahnten Aktualisierung der KpS-Richtlinien liegt ein erster Entwurf der Polizei vor, der noch einer weiteren Abstimmung bedarf.

Der Ausschuss nimmt zur Kenntnis, dass der Senator für Inneres und Sport den Abschluss der Überarbeitung der KpS-Richtlinien bis zum Sommer 2007 zusichert.

Eröffnung des elektronischen Rechtsverkehrs (Ziffer 10.1): Der Ausschuss nimmt zur Kenntnis, dass hinsichtlich der Dauer der Speicherung zwischen dem Senator für Justiz und Verfassung und dem Landesbeauftragten für den Datenschutz vereinbart wurde, in der bereits existierenden Dienstanweisung ergänzend auch die Löschfristen zu beschreiben.

Neues zur elektronischen Gesundheitskarte (Ziffer 11.2): Der Ausschuss nimmt zur Kenntnis, dass das Modellprojekt von den beteiligten Organisationen nicht durchgeführt wird und somit eine Befassung des Rechtsausschusses entbehrlich ist.

Mammographie-Screening (Ziffer 11.3): Das bereits Ende Dezember 2005 vom Landesbeauftragten für den Datenschutz angeforderte Datenschutzkonzept wurde von der „Zentralen Stelle“ des Gesundheitsamtes Bremen Ende Juli 2006 vorgelegt. Darin waren eine Reihe von Punkten überarbeitungsbedürftig: So fehlte eine Beschreibung der Absicherung der Datenbank, ebenfalls nicht enthalten waren Angaben zur Eingabekontrolle und zur Zugriffskontrolle. Darüber hinaus enthielt das an die Frauen gerichtete Einladungsschreiben keinen Hinweis auf die Möglichkeit, der Speicherung ihrer Daten für Zwecke weiterer Einladungen zu widersprechen. Der Vertreter des Gesundheitsamtes Bremen räumte ein, dass im Einladungsschreiben gegenwärtig lediglich auf die Freiwilligkeit einer Teilnahme hingewiesen werde, jedoch ein eindeutiger Hinweis auf die Verweigerungsmöglichkeit fehle und sicherte eine Aufnahme dieses Hinweises für die Zukunft zu. Bei Vorliegen einer Verweigerung der Teilnahme sehe die eingesetzte Software ausdrücklich einen Sperrvermerk mit der Folge vor, dass die persönlichen Daten der Frau gelöscht werden. In diesen Fällen werde die so genannte Screening-ID, ein Sperrgrund und eine Sperrfrist gespeichert. Die Frist ende mit dem Erreichen des siebzigsten Lebensjahres plus zwei Jahre. Danach würden die Daten automatisch komplett gelöscht. Die vom Rechtsausschuss für die Sitzung am 6. Dezember 2006 erbetene abschließende Stellungnahme wurde vom Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales für Ende Januar 2007 angekündigt. Die Stellungnahme liegt noch nicht vor. Der Landesbeauftragte für den Datenschutz hat den Rechtsausschuss in seiner Sitzung am 14. Februar 2007 darüber unterrichtet, dass die „Zentrale Stelle“ mit E-Mail vom 31. Januar 2007 die geforderten Ergänzungen im Datenschutzkonzept vorgenommen habe und die Qualität der einzelnen Maßnahmen vom Landesbeauftragten für den Datenschutz noch geprüft werde. Der Ausschuss nimmt den Sachstand der Bearbeitung zur Kenntnis.

Novellierung des Bremischen Schuldatenschutzgesetzes (Ziffer 13.3): Der Landesbeauftragte für den Datenschutz hat dem Ausschuss mit Schreiben vom 18. Oktober 2006 berichtet, dass mit dem Bildungsressort über den Gesetzentwurf im Jahre 2005 weitgehend Einvernehmen erzielt worden sei und der Gesetzentwurf bereits im Juli 2005 in der Deputation für Bildung beraten worden sei. Vor der Einbringung des Entwurfs in den Senat habe es jedoch von Seiten des Senators für Inneres und Sport Bedenken hinsichtlich der Regelung zur Übermittlung von Schülerdaten an andere öffentliche Stellen gegeben. Inzwischen sei unter den Beteiligten eine einvernehmliche Regelung gefunden worden, mit der bei der Entscheidung zur Datenübermittlung der Erziehungs- und Bildungsauftrag der Schule sowie das Vertrauensverhältnis zwischen Schülerinnen und Schülern und dem Lehrpersonal zu berücksichtigen sei. Der Bürgerschaft (Landtag) liegt mit der Drucksache 16/1216 die Mitteilung des Senats vom 28. November 2006 zur Novellierung zum Bremischen Schuldatenschutzgesetz vor. Der Ausschuss nimmt den Sachstand zur Kenntnis und erklärt den Punkt für erledigt.

Prüfung des Schuldatenverwaltungsverfahrens MAGELLAN (Ziffer 13.4): Der Senator für Bildung und Wissenschaft wies darauf hin, dass Bremen europaweit die erste Region sei, in der dieses Verfahren in der Praxis umgesetzt werde. Im Bereich Bildung kämen im Zusammenhang mit Pisa, Vera und anderen Studien erhebliche Anforderungen auf die Statistik über Schüler, Lehrer und Eltern zu. Weil das Verfahren mit Hilfe einer neuen Software abgewickelt werde, gebe es einen erheblichen Entwicklungsbedarf. Bei 170 Datenbanken seien die Zugriffe zu protokollieren und revisionssicher zu machen. Ungeachtet der durch technische Probleme ein-

getretenen Verzögerungen seien einzelne der mit dem Landesbeauftragten für den Datenschutz im Juni 2006 abgestimmten Maßnahmen inzwischen umgesetzt worden. Der Ausschuss nimmt zur Kenntnis, dass die Verfahrensbeschreibung dem Landesbeauftragten für den Datenschutz zwischenzeitlich vorgelegt wurde und die technische Realisierung – soweit noch ausstehend – durch das Bildungsressort in der unterrichtsfreien Zeit während der Weihnachtsferien 2006/2007 erfolgen wird.

Antrag

Die Bürgerschaft (Landtag) möge beschließen:

Die Bürgerschaft (Landtag) tritt den Bemerkungen des Rechtsausschusses bei.

7.2 Weitere Themen im Ausschuss und im Parlament

Neben der Verabschiedung einer Reihe von Gesetzen mit datenschutzrechtlichen Regelungen oder Aspekten, die im folgenden Teil des Berichts dargestellt werden (vgl. z. B. BremMeldG unter Ziff. 9.1 dieses Berichts), hat sich auf Antrag von SPD und CDU (Drs. 16/1141) die Bürgerschaft (Landtag) für einen verbesserten Datenschutz für ALG-II-Bezieherinnen und -Bezieher eingesetzt. Die Debatte findet sich im Plenarprotokoll der Bürgerschaft (Landtag) vom 16. November 2006, S. 4751 ff. wieder. Hinweisen möchte ich weiterhin auf eine Kleine Anfrage der CDU zum Umgang mit Kontoabfragen durch Finanz- und Sozialbehörden vom 17. Juli 2006 und dazu die Antwort des Senats vom 1. August 2006 (vgl. Drs. 16/1102).

Der Rechtsausschuss der Bürgerschaft hat sich über die obige Darstellungen hinaus u. a. auch noch mit der geplanten Speicherung eines so genannten Kerndatensatzes von Schülern und Lehrern in einer bundesweiten Zentraldatei beschäftigt. Nicht unerwähnt lassen möchte ich an dieser Stelle, dass mir im Berichtsjahr erstmalig im Rahmen der Behandlung meines 27. Jahresberichts (der Stellungnahme des Senats und der Behandlung des Berichts des Rechtsausschusses an die Bremische Bürgerschaft) erlaubt wurde, zu den Abgeordneten des Landtags zu sprechen (vgl. Plenarprotokoll der Bürgerschaft/Landtag vom 23. März 2006, S. 3778 ff.)

8. Personalwesen

8.1 Krankheitsverwaltung im Mitarbeiterportal

Seit ca. zwei Jahren ist in der bremischen Verwaltung durch Erweiterung des PuMa-Verfahrens (Personalverwaltung und -management) das Mitarbeiterportal (MiP) im Einsatz. Über dieses Portal können Mitarbeiter direkt von ihrem PC aus online die Bearbeitung von Urlaubs- und Fortbildungsanträgen sowie die Pflege von persönlichen Daten („Visitenkarte“: Name, Anschriften etc.) vornehmen. Nach Erweiterung des MiP werden krankheitsbedingte Fehlzeiten im DV-Verfahren zur Personalverwaltung (PuMa-Online/MiP) für die Unterstützung der Personalsachbearbeitung zur Ermittlung des Zeitpunktes zur Durchführung des Betrieblichen Eingliederungsmanagements nach § 84 Abs. 2 Sozialgesetzbuch (SGB) IX verarbeitet. In der Protokollerklärung zur Dienstvereinbarung über die Erprobung eines betrieblichen Eingliederungsmanagements ist festgelegt worden, dass darüber hinausgehende Auswertungen nicht zulässig sind. Das Konzept ist mir zur Prüfung vorgelegt worden. Folgende Gesichtspunkte spielen dabei eine Rolle:

Soweit ein Mitarbeiter innerhalb von zwölf Monaten mehr als sechs Wochen krank gewesen ist, greift das Eingliederungsmanagement. Nach der Erweiterung des MiP können Krankmeldungen außer durch den Mitarbeiter selbst auch durch andere Personen oder den Vorgesetzten eingegeben werden. Die Möglichkeit, für einen anderen Kollegen eine Krankmeldung im MiP vorzunehmen, ist jedoch nur mit Einwilligung des Betroffenen zulässig. Es muss daher die Wahlmöglichkeit beibehalten werden, dass ein sich Krankmeldender bei seinem Vorgesetzten bzw. bei der Personalstelle krank meldet und dies dann jeweils von dort in das MiP eingegeben wird.

Außerdem kann der Personalrat auf die Übersicht der Personen zugreifen, die innerhalb eines Jahres mehr als sechs Wochen krank gewesen sind. Da Gesundheitsdaten besondere Arten von Daten nach § 2 Abs. 6 Bremisches Datenschutzgesetz (BremDSG) sind, unterliegen sie einer besonderen Zweckbindung. Ich habe daher darauf hingewiesen, dass dem Personalrat und/oder anderen Personalvertretungen (Vertrauensperson der Schwerbehinderten, Frauenbeauftragte) ein regelmäßiger

bzw. ständiger Zugriff auf Personalaktendaten über Krankheitstage nur mit Einwilligung des Betroffenen ermöglicht werden darf. Dies ergibt sich aus den einschlägigen Rechtsvorschriften für die Personalvertretungen. Angemessen wäre es allenfalls, der Personalvertretung jeweils nur auf Anforderung eine Einsichtsbefugnis in die Übersicht, ggf. auch als Ausdruck, zur Erfüllung ihrer gesetzlichen Aufgaben einzuräumen.

Vorgesehen war auch, die papiergebundene durch eine elektronische Krankheitsakte zu ersetzen. Ich habe darauf hingewiesen, dass dies gegen die Regelung in §§ 93 ff. Bremisches Beamtengesetz (BremBG) verstößt. Darüber hinaus wird weiterhin eine Vielzahl von papiergebundenen Krankenunterlagen nach Ziffer 10 Abs. 3 Nr. 7 Verwaltungsvorschrift über die Erhebung und Führung von Personalaktendaten (PAVwV) vorhanden sein, wie z. B. Arbeitsunfähigkeitsbescheinigungen des Arztes, Unterlagen über Kurverfahren etc., so dass sich dieses Ziel nicht ohne Weiteres verwirklichen lässt.

Der Senator für Finanzen hat meine Änderungsvorschläge übernommen und zugesagt, meine Hinweise zu beachten. Hinsichtlich des Zugriffs der Personalvertretung auf die Daten hat die senatorische Dienststelle mitgeteilt, der Gesamtpersonalrat sei mit meinem Vorschlag nicht einverstanden. Es soll daher ein einvernehmlicher Vorschlag erarbeitet werden, der sowohl den Aufgaben der Interessenvertretungen als auch den Belangen des Datenschutzes Rechnung trägt.

8.2 Neue Dienstvereinbarung über die Nutzung von Telekommunikationsanlagen

Seit mehreren Jahren wird beim Senator für Finanzen über eine neue Infrastruktur der Telekommunikation beraten. An einigen Sitzungen der Arbeitsgruppe habe ich teilgenommen. Ich hatte bereits frühzeitig darauf hingewiesen, dass die Dienstvereinbarung (DV) über die Nutzung von Fernsprechanlagen aus dem Jahre 1991 den zum Teil grundlegend geänderten technischen Anforderungen angepasst werden muss.

Nunmehr ist mir der Entwurf einer neuen DV vorgelegt worden. Er bezieht die neue TK-Infrastruktur ein, die Geltung der Dienstvereinbarung erstreckt sich nun auch auf Mobilfunkgeräte und auf die Sprachübertragung. Unter anderem haben folgende Punkte bei den Beratungen eine Rolle gespielt:

Eine Regelung betraf den Mitschnitt und das unbefugte Mithören von Telefongesprächen. Ich habe vorgeschlagen, in der DV präzise festzulegen, was unter Wahrung der gesetzlichen Bestimmungen erlaubt ist.

Die Zulassung der Funktion „Aufschalten“ hat zu Diskussionen geführt. Technisch gesehen wird mit dieser Funktion einem Dritten ermöglicht, sich in ein laufendes Gespräch zweier Kommunikationspartner einzuschalten, ohne dass dies von einem der beiden Gesprächspartner initiiert wurde. Der Vorgang des Aufschaltens wird zwar durch ein kurzes Tonsignal angekündigt, aber es kann nicht davon ausgegangen werden, dass auch Gesprächsteilnehmer außerhalb der Verwaltung den Ton mit einem Aufschaltvorgang verbinden. Nach der Aufschaltung kann die sich in das Gespräch einschaltende Person beide Teilnehmer hören. Im Entwurf war das Aufschalten von Gesprächen vorgesehen. Ich habe die Streichung empfohlen, weil vertrauliche (nicht nur private) Inhaltsdaten der sich aufschaltenden Person zur Kenntnis gelangen können und insoweit in bestimmten Fällen, z. B. das Beratungsgeheimnis nach § 203 Strafgesetzbuch oder das Fernmeldegeheimnis nach § 88 Telekommunikationsgesetz, verletzt werden können.

Eine weitere bedenkliche Regelung im Entwurf sah vor, bei einer zentralen Administration auf die Protokollierung der Tätigkeiten der Administration zu verzichten, obwohl dies zur nachträglichen Prüfung der Eingabekontrolle erforderlich ist und die Protokolldaten einer strikten Zweckbindung unterliegen.

Inzwischen hat der Senator für Finanzen den Entwurf der DV entsprechend meiner Vorschläge überarbeitet.

Im Rahmen dieser neuen Telekommunikationsstruktur bestand auch die technische Möglichkeit, auf den einzelnen Arbeitsplatz bezogen auszuwerten, wer zu welcher Zeit und wie häufig privat oder dienstlich telefoniert. Nach entsprechender Programmierung ist diese unzulässige Auswertung technisch nicht mehr möglich. Es kann nur noch gruppenbezogen ausgewertet werden. Damit entspricht diese tech-

nische Umgestaltung der Regelung in der DV zur Betriebsdatenverarbeitung und der Regelung, dass eine Leistungs- und Verhaltenskontrolle mit Hilfe von Verkehrsmesseinrichtungen sowie ein Abgleich personenbezogener Daten nicht zulässig ist. Damit ist auch meine Forderung, keine personenbeziehbaren Auswertungen vorzunehmen, erfüllt worden.

9. Inneres

9.1 Änderung des Meldegesetzes

Der Senator für Inneres und Sport bat mich im Berichtsjahr um Stellungnahme zu dem von ihm vorgelegten Entwurf eines Gesetzes zur Änderung des Bremischen Meldegesetzes (BremMeldG). Der Gesetzentwurf sah zahlreiche Änderungen gegenüber dem geltenden bremischen Meldegesetz vor, die überwiegend mit der Notwendigkeit der Anpassung an das Melderechtsrahmengesetz des Bundes und den Auswirkungen des Lebenspartnerschaftsgesetzes begründet wurden. Ziel der Änderung des Meldegesetzes war es darüber hinaus, einen rechtlichen Rahmen für eine rechtsverbindliche Kommunikation unter den Meldebehörden sowie zwischen Bürgerinnen und Bürgern und den Meldebehörden zu schaffen, denn über das Internet soll sich die Verwaltung dem Dialog und der Interaktion mit den Einwohnerinnen und Einwohnern öffnen. Der Gesetzentwurf sah in den folgenden Fällen Regelungen zur Nutzung der elektronischen Kommunikation vor:

— Erteilung von Auskünften an die betroffene Person nach § 9 BremMeldG,

— Erfüllung der allgemeinen Meldepflicht nach § 17 BremMeldG,

— Datenübermittlungen zwischen den Meldebehörden nach § 29 BremMeldG,

— Datenübermittlungen an andere Behörden oder sonstige öffentliche Stellen nach § 30 BremMeldG,

— Datenübermittlungen an öffentlich-rechtliche Religionsgesellschaften nach § 31 BremMeldG und

— Erteilung von einfachen Melderegisterauskünften an Privatpersonen und nicht öffentliche Stellen nach § 32 Abs. 1 BremMeldG.

In meiner Stellungnahme zum Gesetzentwurf machte ich darauf aufmerksam, dass Effizienzsteigerungen durch den zunehmenden IT-Einsatz dort an die Grenze stoßen, wo die schutzwürdigen Interessen des Betroffenen durch die Datenverarbeitung erheblich gefährdet oder beeinträchtigt werden. Bei allen Neuerungen muss daher dem informationellen Selbstbestimmungsrecht des Betroffenen die notwendige Beachtung zukommen. Zur Gewährleistung der an die vorgesehenen Datenübertragungen in elektronischer Form zu knüpfenden Sicherheitsanforderungen und um eGovernment-spezifischen Bedrohungen wirksam begegnen zu können, empfahl ich, Ergänzungen im Gesetzentwurf vorzunehmen. Meinen Empfehlungen entsprechend wurde § 9 Abs. 2 Satz 2 des Entwurfs dahingehend ergänzt, dass bei der Erteilung von Auskünften an die betroffene Person in elektronischer Form über das Internet durch entsprechende Maßnahmen neben der Vertraulichkeit auch die Integrität und die Authentizität der im Melderegister gespeicherten und übermittelten Daten zu gewährleisten ist.

Nach § 32 Abs. 1 a des Entwurfs war vorgesehen, dass einfache Melderegisterauskünfte von den Meldebehörden an Privatpersonen und nicht öffentliche Stellen auch auf automatisiert verarbeitbaren Datenträgern oder durch Datenübertragung (Internet) erteilt werden dürfen. Auf meine Anregung hin wurde hierzu die Bestimmung des nach dem Entwurf vorgesehenen § 32 Abs. 1 b BremMeldG dahingehend ergänzt, dass die Meldebehörde die betroffene Person auf das Recht, der Erteilung einfacher Melderegisterauskünfte über das Internet zu widersprechen, nicht nur vor der Eröffnung des Internet-Zugangs für die Erteilung einfacher Melderegisterauskünfte und bei der Anmeldung des Betroffenen, sondern auch einmal jährlich durch öffentliche Bekanntmachung hinzuweisen hat.

Weitere Verbesserungen des Entwurfs ergaben sich nach meiner Stellungnahme u. a. hinsichtlich der in § 2 BremMeldG geregelten Aufgaben und Befugnisse der Meldebehörde und der Gestaltung des Meldescheins, für die Erfüllung der allgemeinen Meldepflicht nach § 17 BremMeldG und der Anmeldung für Beherbergungsstätten nach § 26 BremMeldG, der nach § 36 BremMeldG nun auch weiterhin eine Rechtsverordnung zu Grunde zu legen ist.

Mit dem Senator für Inneres und Sport zunächst nicht geklärt werden konnten drei wesentliche Kritikpunkte:

— Nach § 3 Abs. 2 Nr. 2 des Entwurfs sollten die Meldebehörden für die Ausstellung von Lohnsteuerkarten künftig auch die „Tatsache des dauernden Getrenntlebens“ bei Verheirateten speichern, was bislang nicht der Fall war. Der Senator für Inneres und Sport begründete die vorgesehene Ergänzung damit, dass die Angabe für die Erstellung der Lohnsteuerkarte von den Meldebehörden benötigt werde.

Ich wies in diesem Punkt darauf hin, dass der Umfang der im Melderegister zu speichernden Daten auf das notwendige Maß zu beschränken sei. Eine Erforderlichkeit für die Aufnahme und Speicherung eines eigenen Merkmals im Melderegister sei nicht erkennbar. Die Aufgabe der Eintragung der Steuerklasse auf der Lohnsteuerkarte könne technisch auch anders gelöst werden und dürfe nicht zu einer fortwährenden Speicherung des dauernden Getrenntlebens durch die Meldebehörde führen. Schließlich können auch bei anderen Steuerklassen, z. B. drei und fünf bzw. vier und vier, Änderungen programmtechnisch dauerhaft angelegt werden, ohne dass hierfür zusätzliche Angaben gespeichert werden müssen.

— Nach § 9 Abs. 7 des Gesetzentwurfs war geplant, dass in den Fällen, in denen einer betroffenen Person die von ihr begehrte Auskunft von der Meldebehörde nicht zu erteilen ist, sie auch nicht dem Landesbeauftragten für Datenschutz und Informationsfreiheit erteilt werden darf, wenn der Senator für Inneres und Sport im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Der Senator für Inneres und Sport verwies zur Begründung dieser Regelung auf die in § 8 Abs. 7 Melderechtsrahmengesetz enthaltene Bestimmung, die in das Bremische Meldegesetz zu übertragen sei, und auf in den allgemeinen Datenschutzgesetzen enthaltene Vorschriften.

Ich erklärte demgegenüber, dass mit der vorgesehenen Regelung in gravierender, nicht akzeptabler Weise in die Kontrollkompetenz des Landesbeauftragten für Datenschutz und Informationsfreiheit eingegriffen würde. Eine effektive unabhängige Kontrolle jeglicher personenbezogener Datenverarbeitung, wie sie vom Bundesverfassungsgericht immer wieder verlangt werde, wäre durch die Vorschrift nicht mehr gewährleistet. Allenfalls hinnehmbar sei eine Formulierung ähnlich dem Bremischen Datenschutz- oder auch Sicherheitsüberprüfungsgesetz, wonach in so gelagerten Fällen eine Auskunft nur dem Landesbeauftragten selbst oder seinem Vertreter nach § 24 Abs. 2 BremDSG zu gewähren ist.

— Nach § 31 Abs. 1 Nr. 11 BremMeldG sollten an die öffentlich-rechtlichen Religionsgesellschaften künftig auch Angaben zu bestehenden Lebenspartnerschaften übermittelt werden dürfen. Zur Begründung verwies der Senator für Inneres und Sport auf Bestimmungen des Melderechtsrahmengesetzes und des Lebenspartnerschaftsgesetzes.

Ich hingegen sah keine praktische Notwendigkeit für eine gesetzlich vorgesehene Übermittlungspflicht dieser besonders sensiblen Daten an die Religionsgesellschaften.

Trotz meiner Kritik erklärte sich der Senator für Inneres und Sport nicht bereit, den Gesetzentwurf in den genannten Punkten zu ändern. Auf meine Intervention in der staatlichen Deputation für Inneres hin beschloss diese, der Senatsvorlage des Senators für Inneres und Sport unter dem Vorbehalt zuzustimmen, im weiteren Gesetzgebungsverfahren klärungsbedürftige Punkte einzubringen bzw. die von mir vorgetragenen Bedenken zu prüfen. So wurde auch verfahren. Nach der ersten Lesung überwies die Bürgerschaft (Landtag) den Gesetzentwurf zur Beratung an den Rechtsausschuss, der auch die Federführung in allen Fragen des Datenschutzes hat. Dort konnte ich erreichen, dass in zwei wesentlichen Punkten Änderungen im laufenden Gesetzgebungsverfahren eingebracht wurden: In § 9 Abs. 7 des Entwurfs wurde eine der im Sicherheitsüberprüfungsgesetz enthaltenen Regelung entsprechende Bestimmung aufgenommen. Auf die nach § 31 Abs. 1 Nr. 11 des Entwurfs vorgesehene Ergänzung wurde zumindest bis zu einer Änderung des Lebenspartnerschaftsgesetzes, aus der sich möglicherweise eine Übermittlungsnotwendigkeit ergibt, verzichtet (Drs. 16/1188). Das Bremische Meldegesetz wurde dann am 21. November 2006 in der geänderten Fassung vom Landtag beschlossen.

9.2 Konsequenzen aus dem Urteil zur Rasterfahndung

Mit Beschluss vom 4. April 2006 (1 BvR 518/02) hat das Bundesverfassungsgericht entschieden, dass eine präventive polizeiliche Rasterfahndung mit dem Grundrecht

auf informationelle Selbstbestimmung (Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 Grundgesetz) nur vereinbar ist, wenn eine „konkrete Gefahr" für hochrangige Rechtsgüter, wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben ist. Im Vorfeld der Gefahrenabwehr scheidet eine solche Rasterfahndung aus. Das Gericht hat weiterhin festgehalten, dass eine allgemeine Bedrohungslage, wie sie im Hinblick auf terroristische Anschläge seit dem 11. September 2001 durchgehend bestanden hat, oder außenpolitische Spannungslagen für die Anordnung der Rasterfahndung nicht ausreichen. Voraussetzung sei vielmehr das Vorliegen weiterer Tatsachen, aus denen sich eine konkrete Gefahr, etwa für die Vorbereitung oder Durchführung terroristischer Anschläge, ergibt. Das Verfassungsgericht betont auch die grundrechtsichernde Bedeutung des Richtervorbehalts und der nachträglichen Benachrichtigung der Betroffenen.

Die Entscheidung, die sich unmittelbar nur mit der Regelung im Polizeigesetz Nordrhein-Westfalen beschäftigt, hat bundesweite Bedeutung, da in Bremen wie auch in allen Polizeigesetzen der anderen Länder Vorschriften zur Rasterfahndung enthalten sind. In Bremen besteht kein aktueller Änderungsbedarf für die Regelung im Bremischen Polizeigesetz (BremPolG). Soweit die Regelung zur Rasterfahndung in § 36 i BremPolG von einer „Gefahr" spricht, ist damit nach der Definition in § 2 Nr. 3 a BremPolG eine „konkrete Gefahr" gemeint.

Auch wenn die Rechtsgrundlage für die Rasterfahndung unter dem o. g. Aspekt einer verfassungsrechtlichen Prüfung standhält, so waren doch die an elf verschiedene Stellen gerichteten Einzelanordnungen der Polizei Bremen und Ortspolizeibehörde Bremerhaven zur Vornahme einer Rasterfahndung im Oktober und November 2001 (vgl. 24. JB, Ziff. 6.3 und 25. JB, Ziff. 6.2) mangels Vorliegens einer konkreten Gefahr mit den Vorgaben des Bundesverfassungsgerichts nicht vereinbar und hätten nicht durchgeführt werden dürfen.

9.3 Maßnahmenkatalog im Terrorismusbekämpfungsergänzungsgesetz

Im Sommer 2006 haben sich die Koalitionsfraktionen und das Bundesministerium des Innern über ein Gesetz zur Ergänzung des aus dem Jahre 2002 stammenden Terrorismusbekämpfungsgesetzes geeinigt, weil dieses Gesetz zum Teil bis zum 11. Januar 2007 befristete Regelungen enthält und dabei eine Evaluierung vor Fristablauf vorsieht. Auf diese Weise soll eine Überprüfung der tiefgreifenden Befugnisnormen sichergestellt werden. Um dem nachzukommen, ist ein Bericht der Bundesregierung zu den Auswirkungen des Terrorismusbekämpfungsgesetzes vorgelegt worden, der die gesetzgeberischen Entscheidungen ganz überwiegend bestätigt, dabei allerdings vorwiegend eine quantitative Analyse der Anwendung der neuen Maßnahmen vornimmt, ohne die betroffenen Grundrechtspositionen mit einzubeziehen. Zudem handelt es sich nicht um einen wissenschaftlich abgesicherten Bericht.

Die wesentlichen Punkte des Gesetzentwurfs (BT-Drs. 16/2921 vom 12. Oktober 2006) sind:

— die Befugnisse des Terrorismusbekämpfungsgesetzes werden um fünf Jahre verlängert;

— Auskunftsrechte etwa gegenüber Post- und Telekommunikations- sowie Teledienstleistern, Luftfahrtunternehmen und Finanzdienstleistungsunternehmen, die bisher nur dem Bundesamt für Verfassungsschutz zur Verfügung standen, werden auf den Bundesnachrichtendienst und den Militärischen Abschirmdienst ausgedehnt;

— bestehende Befugnisse der Nachrichtendienste, Auskünfte einholen zu können, werden zur Aufklärung verfassungsfeindlicher Bestrebungen im Inland erweitert;

— IMSI-Catcher zur Gewinnung von Telefonverbindungsdaten dürfen eingesetzt werden;

— den Nachrichtendiensten wird die Ausschreibung von Personen im Schengener Informationssystem eröffnet;

— die Nachrichtendienste können künftig Auskünfte aus dem Zentralen Fahrzeugregister abrufen;

— die zollamtliche Sicherstellung bei Geldwäscheverdacht wird auf Fälle des Terrorismusfinanzierungsverdachts übertragen.

Auf seiner Sitzung am 1. Dezember 2006 hat der Deutsche Bundestag das Gesetz unter Berücksichtigung des Berichts des Innenausschusses (BT-Drs. 16/3642), u. a. mit kurzfristigen Änderungen des Passgesetzes zur Vorbereitung der Aufnahme von Fingerabdrücken in den Pass, angenommen.

Aus Sicht des Datenschutzes wirft das Gesetz eine Reihe von Fragen auf, beginnend damit, dass keine unabhängige und wissenschaftlich begleitete Evaluierung der Gesetzesfolgen vorgenommen wurde. Die 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hieraus mit ihrer Entschließung (vgl. Ziff. 19.8 dieses Berichts) die Schlussfolgerung gezogen, dass damit „sowohl die Notwendigkeit einer Verlängerung als auch die Erforderlichkeit der Schaffung neuer Befugnisse in Zweifel steht". Das Gesetz steht auch im Widerspruch zu verfassungsgerichtlichen Entscheidungen, etwa den Beschluss des Bundesverfassungsgerichts vom 4. April 2006 zur Rasterfahndung oder zur präventiven Wohnraumüberwachung vom 3. März 2004, die wiederholt auf die engen Grenzen von Vorfeldmaßnahmen hingewiesen haben, die allein der Gewinnung von Verdächtigen dienen. Das Gesetz vom 5. Januar 2007 (BGBl. I S. 2) ist inzwischen in Kraft getreten.

9.4 Antiterrordatei-Gesetz

Seit 2001 wird zwischen den Innenministern von Bund und Ländern die Einrichtung einer Antiterrordatei diskutiert. Strittig waren dabei u. a. Inhalt und Struktur der Datei sowie die Eingabe- und Abrufrechte von Daten. Im Jahr 2004 mündeten die Überlegungen, eine gemeinsame Datei der deutschen Sicherheitsbehörden zur Beobachtung und Bekämpfung des islamistischen Extremismus und Terrorismus aufzubauen, in einen vom Bundesrat getragenen Gesetzentwurf (BT-Drs. 15/4413). Die Bundesratsinitiative hatte im Ergebnis keinen Erfolg, auch aufgrund der ungeklärten Rechtsfragen zur Zusammenarbeit zwischen Verfassungsschutzbehörden und Polizei.

Innerhalb der Bundesregierung wurde die Thematik jedoch in Bezug auf die Bekämpfung des internationalen Terrorismus weiter verfolgt. Im Sommer 2006 wurde schließlich der Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder vorgelegt und nach Abstimmung mit den Ländern Mitte Oktober 2006 in den Bundestag eingebracht (BT-Drs. 16/2950) und dort am 1. Dezember 2006 in der Fassung der Beschlussempfehlung und des Berichts des Innenausschusses (BT-Drs. 16/3642) beschlossen (BR-Drs. 893/06).

Meine Bedenken gegen den mir auf Anfrage im Sommer 2006 vom Senator für Inneres und Sport zur Verfügung gestellten Gesetzentwurf habe ich diesem im August 2006 mitgeteilt. Die Vorschläge haben jedoch bei der Abstimmung des Gesetzentwurfs auf Länderebene keinen Eingang gefunden. Der Gesetzentwurf wurde im Gegenteil erheblich verschärft. So ist es z. B. den einstellenden Behörden erlaubt, in Freitextfeldern eigene Einschätzungen und Bewertungen abzugeben, die eine Vielzahl auch so genannter weicher personenbezogener Informationen enthalten, z. B. nicht überprüfte Hinweise oder Vermutungen ohne Bindung an hinreichend konkrete Festlegungen, und auf die die am Verbund teilnehmenden Behörden zugreifen können. Zudem besteht eine Eilfallregelung, bei der die Sicherheitsbehörden, vor allem die Polizei, einen Vollzugriff auch auf nachrichtendienstliche Informationen erlangen. Es ist zweifelhaft, ob bei dieser Qualität der Zusammenarbeit das Trennungsgebot zwischen polizeilicher Exekutivgewalt und nachrichtendienstlicher Informationssammlung noch gewahrt bleibt. Ferner wurde der Umfang der in der Antiterrordatei zu speichernden Daten und Personen, insbesondere der Kontakt- und Begleitpersonen, die durch auf legalem Verhalten oder unverdächtigem sozialen Verhalten beruhenden Anhaltspunkten erfasst werden können, und der Umfang der abfrageberechtigten Behörden in bedenklichem Umfang erweitert.

Aus Sicht der Datenschutzbeauftragten des Bundes und der Länder enthält das Gesetz erhebliche schwerwiegende verfassungs- und datenschutzrechtliche Risiken. Auf der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 2006 haben die Datenschutzbeauftragten in einer Entschließung die Beachtung verfassungsrechtlicher Grundsätze, insbesondere des Rechts auf informationelle Selbstbestimmung, des Grundsatzes der Verhältnismäßigkeit und des Trennungsgebots angemahnt (vgl. Ziff. 19.9 dieses Berichts). Das Gesetz vom 30. Dezember 2006 (BGBl. I S. 3409) ist inzwischen in Kraft getreten.

9.5 Discomeile

9.5.1 Razzia der Polizei Bremen in der Diskothek „Stubu“

In der Nacht vom 27. zum 28. August 2006 hat die Polizei Bremen in einer groß angelegten Razzia das Tanzlokal „Stubu“ und angrenzende Räume durchsucht. Von den dabei angetroffenen 1.500 Besuchern wurden die Personalien festgestellt, es erfolgte eine Abfrage im Fahndungsbestand der Polizei und verschiedentlich eine körperliche Durchsuchung. Hierfür wurden die Besucher in Gruppen nach und nach abgeführt und in Räumlichkeiten u. a. des Finanzamtes Bremen-West gebracht. Hier hatte die Polizei Bremen insgesamt 40 Arbeitsplätze auf drei Etagen eingerichtet. Die verwendeten Räume betrafen drei Sachgebiete des Finanzamtes, u. a. den Kassenbereich und die Veranlagung.

Nach § 7 Abs. 4 Bremisches Datenschutzgesetz (BremDSG) haben öffentliche Stellen, die personenbezogene Daten verarbeiten, technische und organisatorische Maßnahmen zu treffen, um deren Schutz zu gewährleisten. Der Schutzumfang richtet sich u. a. nach dem Umfang und der Sensibilität der verarbeiteten personenbezogenen Daten. Im Finanzamt werden in großem Umfang besonders sensible personenbezogene Daten verarbeitet, die dem Steuergeheimnis (§ 30 Abgabenordnung) unterliegen. Schutzziel der technisch-organisatorischen Maßnahmen ist u. a., Unbefugten den Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zutrittskontrolle), zu verhindern, dass eine Nutzung durch Unbefugte erfolgt (Zugangskontrolle) sowie zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle).

Es ist bedenklich, wenn eine Vielzahl von Polizeibeamten und Diskothekenbesucher sich über einen mehrstündigen Zeitraum in den Räumen des Finanzamtes aufgehalten haben, in denen sich Steuerunterlagen befinden. Die Anwesenheit einer Vielzahl finanzamtsexterner Personen in den Räumen des Finanzamtes erhöht das Risiko einer unbefugten Kenntnisnahme oder des Verlustes von Steuerdaten beträchtlich.

Vor diesem Hintergrund wäre es erforderlich gewesen, ergänzende Sicherheitsmaßnahmen zu treffen, um dieser Risikoerhöhung entgegenzuwirken und das im Datenschutzkonzept niedergelegte Sicherheitsniveau aufrecht zu halten, etwa durch Anwesenheit von Finanzamtsmitarbeitern, das vorherige Verbringen aller Akten mit personenbezogenen Angaben in verschlossene Schränke sowie ein Ausweichen der Polizei in Räume, z. B. Besprechungsräume, in denen keine personenbezogenen Daten gelagert werden.

Ich habe mich daher zum einen an die Polizei Bremen gewandt, um festzustellen, welche Daten erhoben und wie diese weiterverarbeitet worden sind und zum anderen an das betroffene Finanzamt, um zu klären, zu welchem Zeitpunkt und in welchem Umfang das Finanzamt im Vorfeld von der Polizei Bremen bzw. dem Senator für Finanzen über die Inanspruchnahme der Räumlichkeiten informiert worden ist, und welche Maßnahmen daraufhin veranlasst worden sind, um einen angemessenen Schutz personenbezogener Daten, insbesondere von Daten, die dem Steuergeheimnis unterliegen, sicherzustellen.

Meine Anfrage ist vom Finanzamt Anfang Oktober 2006 an den Senator für Finanzen weitergeleitet worden. Eine Antwort steht derzeit noch aus. Bei der Polizei Bremen konnte ich feststellen, dass keine eigenständige Datei errichtet wurde und die Daten nur in geringem Umfang, soweit ein Tatverdacht bestand, zur Anfertigung von Anzeigen und Speicherungen im polizeilichen Informationssystem geführt haben.

9.5.2 Zuverlässigkeitsüberprüfungen von Türstehern von gastgewerblichen Diskotheken

Die Ankündigung des Senators für Inneres und Sport Ende Januar 2006, zur Befriedung der „Discomeile“ hätten sich Türsteher einer Zuverlässigkeitsüberprüfung wie im privaten Sicherheitsgewerbe zu unterwerfen, habe ich zum Anlass genommen, mich bei der Polizei Bremen über das geplante Vorgehen zu erkundigen.

Anfang Februar 2006 wurde mir mitgeteilt, zur Beschleunigung und Vereinfachung der Zuverlässigkeitsüberprüfung sei geplant, die Türsteher um eine schriftliche Einverständniserklärung zur Weitergabe ihrer bei der Polizei Bremen gespeicherten Daten an die jeweiligen Diskothekenbetreiber zu bitten. Es erfolge zunächst eine

Einzelfallprüfung durch die Polizei, aus der sich eine Gesamtprognose mangelnder Zuverlässigkeit ergeben könne. Diese Gesamtprognose sollte dem Diskothekenbetreiber mitgeteilt werden. Zugleich wurde der Entwurf des hierfür vorgesehenen Formulars übermittelt.

Ich hatte datenschutzrechtliche Bedenken sowohl gegen die inhaltliche Ausgestaltung des Formulars als auch die Vorgehensweise, und habe diese der Polizei Bremen umgehend mitgeteilt.

Ich wies auf die bestehenden Möglichkeiten einer Zuverlässigkeitsüberprüfung nach der Gewerbeordnung in Verbindung mit der Bewachungsverordnung sowie nach dem Gaststättenrecht hin, für die das Stadtamt Bremen zuständig sei. Da insoweit eine Rechtsgrundlage besteht, bedarf es keiner Einwilligung der Betroffenen. Für ein zusätzliches Zuverlässigkeitsüberprüfungsverfahren der Polizei Bremen sei neben diesen vorhandenen Möglichkeiten kein Raum. Wie bereits beim Akkreditierungsverfahren zur Fußball-WM 2006 ausgeführt, stehe ich Zuverlässigkeitsüberprüfungen auf Einwilligungsbasis generell ablehnend gegenüber. In aller Regel fehlt es an einer wirksamen Einwilligungserklärung, da die Betroffenen, so auch hier, ihr Einverständnis im Rahmen ihres Beschäftigungsverhältnisses faktisch nicht „freiwillig“ abgeben. Zudem war nach dem mir vorliegenden Formular auch ein informiertes Einverständnis nicht möglich, da der Umfang der Datenverarbeitung, insbesondere welche Daten verarbeitet werden und unter welchen Umständen es zu einer negativen Gesamtprognose kommt, nicht im Ansatz erläutert wurde. Problematisch war zudem aus Rechtsschutzgründen die Weitergabe der Prognose an den Diskothekenbetreiber, ohne den Betroffenen vorab die Möglichkeit zu geben, unrichtige Angaben berichtigen, sperren oder löschen zu lassen.

Die Polizei Bremen nahm dann Abstand von der vorgesehenen Einverständniserklärung. Tätig wurde das Stadtamt Bremen, das nach Gaststättenrecht eine fehlende Zuverlässigkeit der in den Diskotheken Beschäftigten, vor allem der Türsteher, überprüfte. Im Rahmen dieser Überprüfung wirkte die Polizei Bremen durch Übermittlung von Angaben aus dem polizeilichen Informationssystem mit. Die Überprüfung führte in einer Reihe von Fällen zur Annahme der Unzuverlässigkeit der Beschäftigten. Das Stadtamt Bremen forderte von dem Betreiber der Diskothek deren Entlassung und begründete später auch einen beabsichtigten Entzug der Gaststättenlizenz u. a. mit der Unzuverlässigkeit bestimmter Mitarbeiter.

9.5.3 Videoüberwachung der Discomeile

Im Anschluss an die Schießerei auf der so genannten Discomeile entnahm ich der Presse Überlegungen der Polizei Bremens und des Senats, die Discomeile mit Videokameras zu überwachen. Auf meine Anfrage bei der Polizei Bremen Anfang Februar 2006 wurde mir schließlich Ende Juli 2006 ein dreiseitiger Vermerk zu einer Ortsbesichtigung im Mai 2006 und das Richtpreisangebot eines Unternehmens mit der Bitte um Stellungnahme übersandt.

Anfang August 2006 habe ich zu den mir bekannten Unterlagen Stellung genommen. Mangels technischen Konzepts, insbesondere der Vernetzung der Komponenten und der Übertragungswege, war dies aus technischer Sicht nur eingeschränkt möglich. Aus rechtlicher Sicht habe ich angemerkt, dass der technischen Ausgestaltung („wie“) eine Entscheidung über das „ob“ der Maßnahme vorauszugehen hat und auf die Anforderungen des § 29 Abs. 3 Bremisches Polizeigesetz (BremPolG) hingewiesen. Insbesondere fehlten Unterlagen zur erhöhten Kriminalitätsbelastung und zum Ausscheiden anderer Maßnahmen, wie eine verstärkte Polizeipräsenz. Zudem wies ich auf Einschränkungen bei der Videoüberwachung in zeitlicher, örtlicher und technischer Sicht hin, die sich aus dem Grundsatz der Verhältnismäßigkeit ergeben können. Ich wies ferner auf die fehlende örtliche Abgrenzung der Discomeile hin sowie das Verbot, anliegende Wohnhäuser und private Zufahrten, Geschäftshäuser und den angrenzenden Verkehr auf der Hochstraße zu überwachen.

Anfang November 2006 übersandte mir die Polizei Bremen verschiedene Tabellen zur Kriminalitätsbelastung einzelner Straßen in Bremen. Der Rembertiring als Teil der Discomeile befand sich, je nach Deliktart, in einer größeren oder kleineren Spitzengruppe.

Mitte Dezember kam es aufgrund der fortgeschrittenen Planungen zu einem weiteren Gespräch bei der Polizei Bremen, in der diese nähere Aussagen zur technischen Gestaltung und Übermittlung der Daten an die Polizei Bremen traf. Neben

meinen bisherigen Anmerkungen habe ich vor allem Bedenken hinsichtlich einer 24-Stunden-Überwachung geltend gemacht. Die Videoüberwachung stellt einen besonders intensiven Eingriff in das Recht auf informationelle Selbstbestimmung dar und darf nur unter engen Voraussetzungen eingesetzt werden. Hierzu gehört insbesondere der Nachweis eines Kriminalitätsschwerpunktes, der zu allen Zeiten der Überwachung vorhanden sein muss. Sofern vormittags oder tagsüber die Discomeile als öffentlich zugänglicher Ort keine erhöhte Kriminalitätsbelastung aufweist, fehlt die Notwendigkeit einer Videoüberwachung. Dies liegt auch im Interesse der Polizei, da eine 24-Stunden-Überwachung der Videokameras deutlich mehr Personal bindet. Die am Wochenende oder in den Abend- und Nachtstunden im Zusammenhang mit dem Besuch von Diskotheken anzutreffende Kriminalität ist ferner zeitlich fixiert, so dass beim zeitweisen Abschalten der Videoüberwachung tagsüber innerhalb der Woche weder ein Ausweich- noch Verdrängungseffekt zu erwarten ist.

Die Polizei Bremen kündigte an, mich im weiteren Verlauf rechtzeitig über die Planungen zu unterrichten.

9.5.4 Datei Türsteher/Rocker

Aufgrund des erhöhten Kriminalitätsaufkommens, der Gewaltbereitschaft und der Verbindungen zur organisierten Kriminalität dieses Personenkreises führt die Polizei Bremen eine Arbeitsdatei Türsteher/Rocker.

Nach Durchsicht der Verfahrensbeschreibung hatte ich eine Reihe Kritikpunkte. Der Zweck der Datei und damit die Zweckbindung der erhobenen Daten war unklar gefasst. Die angeführten Rechtsgrundlagen für die Erhebung waren nicht zutreffend. Es wurden Daten erhoben, deren Erforderlichkeit für die Sachbearbeitung nicht erkennbar war. Zudem bestand die Möglichkeit, in einem Freitextfeld unkanalisiert weitere Anmerkungen vorzunehmen. Die technischen und organisatorischen Maßnahmen waren unzulänglich dargestellt. Anfang September 2006 habe ich mich bei der Polizei Bremen über die Anwendungspraxis der Datei informiert.

Dabei musste ich feststellen, dass die technischen und organisatorischen Maßnahmen aus einer anderen Verfahrensbeschreibung übernommen worden waren, jedoch tatsächlich nicht zutrafen. Damit konnte auch die gesetzlich vorgesehene Vorabkontrolle unter Einbeziehung des behördlichen Datenschutzbeauftragten im Vorfeld nicht ordnungsgemäß stattgefunden haben. Hierauf habe ich den behördlichen Datenschutzbeauftragten hingewiesen. Ich stellte vor Ort auch fest, dass zwei Mitarbeiter, die früher einmal berechtigt waren, mit der Datei zu arbeiten, nunmehr aber anderen Aufgabengebieten zugewiesen waren, weiter zugriffsberechtigt waren. Zudem konnte auf Betriebssystemebene ein weiterer nicht berechtigter Mitarbeiter Zugriff auf die Daten nehmen. Etwaige Zugriffe wurden nicht protokolliert. Den Entzug dieser Zugriffsberechtigungen habe ich im September 2006 angemahnt.

Anfang Dezember 2006 teilte mir die Polizei Bremen mit, dass eine Überarbeitung der Verfahrensbeschreibung einschließlich der technischen und organisatorischen Maßnahmen noch nicht erfolgen konnte. Dazu habe ich weiter aufgefordert.

9.6 Datenbank TOP-Täter

Anfang September 2006 habe ich die Polizei Bremen über meine datenschutzrechtlichen Bedenken beim Betrieb der Datenbank TOP-Täter unterrichtet. Die Datenbank führt über Intensivtäter Angaben aus den polizeilichen Systemen ISAWeb und INPOL sowie dem Meldewesenverfahren MESO zusammen. Diese Daten sollen einer besonderen Analyse zugeführt werden, um gezielte Einzelmaßnahmen vornehmen zu können. Die mir übersandte Verfahrensbeschreibung wies erhebliche formale und inhaltliche Defizite auf. Daraufhin habe ich mir kurzfristig den Betrieb der Datenbank bei der Polizei Bremen angeschaut.

Dabei stellte ich fest, dass die Zusammenführung und Pflege der Daten manuell erfolgt und der Datenbestand zum Zeitpunkt der Prüfung nicht aktuell war. Es erfolgte auch keine Protokollierung der Eingaben, so dass missbräuchliche Veränderungen oder Löschungen nicht aufgedeckt hätten werden können. Ferner stellte ich fest, dass über das Intranet der Polizei auf die Datenbank zugegriffen werden kann und damit auch bei der Polizei Bremen Beschäftigte, die diese Daten nicht zu dienstlichen Zwecken benötigen, Zugriff nehmen können. Es konnten keine Angaben zu weiteren technischen und organisatorischen Maßnahmen, insbesondere der Zugriffs-, Weitergabe- und Verfügbarkeitskontrolle gemacht werden.

Auch steht nicht fest, nach welchen Kriterien Intensivtäter definiert sind, obwohl diese Einstufung mit gravierenden Folgen für die Betroffenen verbunden ist. Insoweit wirkt sich auch die angestrebte lediglich zweimonatige Aktualisierung aus, die zudem nicht eingehalten wird. Auch war vorgesehen, alle Ordnungswidrigkeiten der Betroffenen einzuspeichern, obwohl dies mit Ziffer 2.4 der Richtlinien für Kriminalpolizeiliche Sammlungen (KpS) nicht vereinbar ist. Erhoben und gespeichert werden sollte zudem eine Reihe von Daten, deren Verarbeitung bedenklich bis absolut unzulässig ist, z. B. Angaben zu Ex-Lebenspartnern und Freunden, die Höhe der Sozialleistungen, Auszahlungszeiträume, -termine und weitere Erkenntnisse des Sozial-, Arbeits- oder Jugendamtes, ferner Erziehungsmaßnahmen innerhalb der Schule, die Zugehörigkeit zu Vereinen und Angaben von Vorgesetzten und das Arbeitsgehalt, beantragte Fahrprüfungen nebst Ergebnis und medizinisch/psychologische Untersuchungen, Angaben zu Fahrzeugen von Familienmitgliedern und Freunden, schließlich Vermutungen zur Motivlage und Angaben zur Persönlichkeit (ethnische Herkunft, Glaubensrichtung, Wertevorstellung).

Als Einzelfallmaßnahme war u. a. eine Gefährderansprache in der Wohnung oder in ähnlichen Rückzugsräumen vorgesehen, „um in die Intimsphäre gelangen zu können". Insoweit wurde der unantastbare Kernbereich der privaten Lebensgestaltung ignoriert. Schließlich sollten die Betroffenen für die Gefährderansprache auch aus dem Unterricht geholt werden oder die Ansprache in Anwesenheit des Lehrers, älteren Bruders, Imams oder anderer Respektpersonen erfolgen können, ohne dass für diese Datenübermittlung eine Rechtsgrundlage zutraf.

Mit Schreiben vom 23. November 2006 teilte mir die Polizei Bremen mit, dass die Datenbank nicht weitergeführt wird, über das Intranet nicht mehr erreichbar sei und die Daten in der Datei gelöscht wurden.

9.7 Datei Straßendeal

Durch die Mitteilung des Senats zum öffentlich wahrnehmbaren Drogenhandel im Land Bremen (Drs. 16/968) bin ich auf die dort angeführte Datei Straßendeal und die Datei Platzverweise aufmerksam geworden, in denen Anhaltemeldungen und Platzverweise aufgenommen werden. Da in beiden polizeilichen Dateien nach der Darstellung des Senats personenbezogene Daten gespeichert werden, bedarf es nach § 36 j Bremisches Polizeigesetz (BremPolG) in Verbindung mit § 8 Bremisches Datenschutzgesetz (BremDSG) einer Datei- bzw. Verfahrensbeschreibung. Diese habe ich am 7. August 2006 angefordert und Anfang September im Rahmen eines Besuchs bei der Polizei Bremen erinnert.

Die Polizei Bremen hat mir Anfang November 2006 mitgeteilt, mich in Kürze über die Verfahrensbeschreibung zu informieren. Auf erneute Anfrage wurde mir Anfang Dezember 2006 mitgeteilt, dass die Einrichtung einer Datei Straßendeal einmal geplant gewesen sei, aus technischen Gründen das Vorhaben jedoch nicht realisiert werden konnte. Im Ergebnis bedeutet dies scheinbar, dass die in der Mitteilung des Senats zum öffentlich wahrnehmbaren Drogenhandel im Land Bremen getätigten Aussagen insoweit nicht zutreffen.

Drogendealer werden jedoch, sofern sie einen Platzverweis erhalten, in die im Zusammenhang mit dem polizeilichen Informationssystem ISAWeb bestehende Rubrik Platzverweise eingetragen. Dies ist zur Kontrolle der Einhaltung von Platzverweisen nach dem BremPolG erforderlich und daher nicht zu beanstanden.

9.8 Alkohol-Datei Jugend ohne Promille

Aufgrund von Presseberichten habe ich mich im Januar 2006 an die Polizei Bremen gewandt und nach der Rechtsgrundlage und Ausgestaltung der Datei Jugend ohne Promille erkundigt. In der Datei sollen von der Polizei Bremen auffällige Jugendliche im Zusammenhang mit alkoholbedingten Gewalttaten erfasst werden.

Die von der Polizei Bremen übermittelte Verfahrensbeschreibung besaß verschiedene Defizite. Daraufhin habe ich die Datei bei der Polizei Bremen eingesehen. Mit Schreiben vom August 2006 habe ich verschiedene verfahrensmäßige und inhaltliche Vorgaben für den weiteren Betrieb der Datei formuliert, u. a. Einschränkungen bei der Datenerhebung und Zweckbestimmung sowie die Angabe der korrekten Rechtsgrundlagen. Daneben habe ich Ergänzungen bei den technisch-organisatorischen Maßnahmen, etwa der Zugriffs-, Weitergabe- und Eingabekontrolle angemahnt. Anfang Oktober 2006 habe ich an deren Umsetzung erinnert. Anfang De-

zember 2006 hat die Polizei mitgeteilt, dass sie alle meine Anforderungen umsetzen wird. Eine angepasste Verfahrensbeschreibung ist mir bislang nicht übersandt worden.

9.9 Stellungnahmen zu Errichtungsanordnungen im Bereich der Polizei

Im Jahr 2006 bin ich aufgefordert gewesen, zu wenigstens 33 Errichtungsanordnungen neuer oder veränderter personenbezogener Sammlungen beim Bundeskriminalamt, auf die auch die Polizei Bremen zugreift, gegenüber dem Senator für Inneres und Sport Stellung zu nehmen. Ich konnte nicht zu allen Anordnungen Stellung nehmen; oft ging es um ungenaue Formulierungen, die zu Schwierigkeiten bei der Anwendung geführt hätten.

9.10 Datei Hafensicherheit

Über die Datei Hafensicherheit wird die Beteiligung der Polizeibehörden des Landes Bremen an den Zuverlässigkeitsüberprüfungen nach dem Hafensicherheitsgesetz abgewickelt. Die mir seitens der Polizei Bremen vorliegende Dateibeschreibung aus dem Jahr 2004 war mit verschiedenen Mängeln behaftet. Ich habe mich daher im September 2006 über die Anwendungspraxis vor Ort informiert und mehrere Mängel bei der Zugriffs- und Eingabekontrolle vorgefunden. Daraufhin habe ich aus rechtlicher und technischer Sicht aufgefordert, Änderungen zu folgenden Punkten vorzunehmen:

Die in der Dateibeschreibung angeführten Rechtsvorschriften waren teilweise unzutreffend und nicht vollständig wiedergegeben, insbesondere fehlten Durchführungsregelungen zur Berichtigung, Sperrung und Löschung personenbezogener Daten. Eine Reihe von Daten sollte erhoben werden, die für den Zweck der Überprüfung der Zuverlässigkeit nach dem Hafensicherheitsgesetz nicht erforderlich waren, etwa zum Alter und Aufenthaltsort sowie zur Staatsangehörigkeit und Volkszugehörigkeit. Es fehlten Angaben zur Speicherdauer sowie zu den technischen und organisatorischen Maßnahmen, vor allem der Zugriffs-, Weitergabe-, Eingabe- und Verfügbarkeitskontrolle.

Die Polizei Bremen hat die von mir vorgeschlagenen rechtlichen Änderungen zwischenzeitlich vorgenommen. Eine Anpassung der technischen und organisatorischen Maßnahmen soll mit der Erstellung des Rahmendatenschutzkonzepts erfolgen. Ich habe die Polizei Bremen darauf hingewiesen, dass dies nicht ausreichend ist, da es sich um verfahrensspezifische Änderungen handelt, die nicht vom Rahmendatenschutzkonzept erfasst werden.

9.11 Eingaben im Bereich der Polizei

Im Berichtsjahr erreichte mich eine Reihe von Anfragen und Beschwerden, die verschiedene Aspekte der Arbeit der Polizei betrafen. Einige seien hier näher beschrieben.

Mehrere Bürger wandten sich an mich, um Auskunft über die zu ihrer Person im polizeilichen Informationssystem gespeicherten Daten zu erlangen oder diese im Anschluss daran berichtigen oder löschen zu lassen. Im Einzelfall schwierig gestaltet sich dabei der Umfang der von der Polizei gespeicherten Daten und die Dauer der Aufbewahrung. So speichert die Polizei in bestimmten Fällen zur Eigensicherung der Beamten zu Betroffenen so genannte personengebundene Hinweise (PHW), z. B. gewalttätig, bewaffnet oder psychisch auffällig. Der Umgang mit diesen PHW, insbesondere die Vergabe und die Löschfristen, ist nicht immer eindeutig. Ein weiteres Problem in der Praxis ergibt sich aus fehlenden Rückmeldungen zum Verfahrensausgang. Dieser ist bedeutsam für die Dauer der Speicherung, die z. B. bei Freispruch, Einstellung mangels Beweisen und Verurteilung variiert, aber auch für das Delikt, das sich zwischen Anzeige bei der Polizei, Ermittlung bei der Staatsanwaltschaft und richterlicher Würdigung ändern kann und ebenfalls Einfluss auf die Speicherdauer hat. In einigen Fällen sind unstrittige Löschungen ausgeblieben und erst aufgrund meiner Anfrage anlassbezogen nachgeholt worden. Die Löschung einzelner Einträge kann zudem dazu führen, dass die zulässige Speicherdauer vorangehender Einträge überschritten wird und diese in der Folge ebenfalls zu löschen sind. Unzulässige Ein- oder Fortspeicherungen können, wie mir berichtet wurde, bei Online-Personalienkontrollen durch Polizeibeamte einen verfälschten Eindruck der Person vermitteln und dadurch zu ungerechtfertigten Maßnahmen führen, z. B. Verbringen auf die Wache und Drogentests.

Auch bin ich in Fällen tätig geworden, in denen der Verdacht bestand, dass Informationen aus dem polizeilichen Informationssystem von Beamten zu privaten Zwecken abgerufen und verwendet wurden. Dabei sind Protokollauswertungen ein wichtiges Hilfsmittel. Sofern der Verdacht sich erhärtete, habe ich Untersuchungen der Innenrevision und dienstrechtliche Konsequenzen gefordert. In einem Fall sind weitergehende strafrechtliche Ermittlungen wegen des Verdachts des Verrats von Dienstgeheimnissen eingeleitet worden.

Daneben haben sich Bürger z. B. in einem Fall beschwert, dass innerhalb der Polizei Bremen eine Galerie von Blitzerfotos existiert, die auf meine Bitte beseitigt wurde. In einem Fall besteht der Verdacht, dass die Polizei in überwachungsfreie Telefongespräche eines Verteidigers mit seinem Mandanten hineingehört hat, in einem anderen Fall, dass Angaben aus dem polizeilichen Informationssystem unzulässigerweise Zeugen im Rahmen der Vernehmung vorgehalten wurden. Die Untersuchungen in beiden Fällen dauern noch an.

Daneben haben sich auch Beamte der Polizei sowie andere öffentliche und nicht öffentliche Stellen an mich gewandt und in verschiedenen Konstellationen eine datenschutzrechtliche Bewertung der Erhebung von personenbezogenen Daten eingeholt, z. B. durch die Polizei bei Krankenkassen oder Wohnungsunternehmen, der Übermittlung von polizeilichen Informationen an Private, z. B. zur Verfolgung von zivilrechtlichen Ansprüchen, oder um Hilfe bei der Auslegung von Datenschutzvorschriften gebeten, etwa den Strafvorschriften des Bremischen Datenschutzgesetzes oder des Bundesdatenschutzgesetzes.

9.12 Neufassung der KpS-Richtlinien

In meinem 28. Jahresbericht (vgl. Ziff. 9.7) hatte ich gefordert, dass die Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien) zu aktualisieren sind. Die zurzeit gültigen Richtlinien aus dem Jahr 1981 sind veraltet und entsprechen nach 25 Jahren zum Teil nicht mehr den derzeit geltenden Rechtsvorschriften. Anfang März 2006 habe ich mich an den Senator für Inneres und Sport gewandt und erfragt, ob meine Einschätzung, dass eine Überarbeitung geboten sei, geteilt wird und ob hierfür bereits Vorarbeiten oder konkretisierte Vorstellungen bestehen. Da ich keine Antwort erhielt, wiederholte ich mein Anliegen Anfang Mai 2006. Daraufhin wurde mir vom Senator für Inneres und Sport mitgeteilt, dass an einem Entwurf zur Neufassung der KpS-Richtlinien gearbeitet werde. Sobald der Entwurf fertiggestellt und geprüft worden sei, werde ich beteiligt.

In seiner Stellungnahme auf meinen 28. Jahresbericht (Drs. 16/1111) teilte der Senat im August 2006 mit, die notwendige Aktualisierung der KpS-Richtlinien sei weitestgehend abgeschlossen und befinde sich in der internen Abstimmung. Sobald diese abgeschlossen sei, erfolge eine Übermittlung an mich. Da mir ein weitestgehender Abschluss der Aktualisierung unbekannt war, bat ich um Aufklärung. Im November 2006 bekräftigte der Senator für Inneres und Sport im Rechtsausschuss, die Aktualisierung sei weitestgehend abgeschlossen.

In der Folgezeit stellte sich heraus, dass ein erster Entwurf der Polizei vorlag, der noch weiterer Abstimmung bedurfte. Der Senator für Inneres und Sport sicherte den Abschluss der Überarbeitung durch sein Haus bis zum Sommer 2007 zu.

9.13 Datenübermittlung des LKA an das BKA im Fall Murat Kurnaz

Im Zusammenhang mit dem in Bremen lebenden Guantanamo-Häftling Murat Kurnaz wurde über die Presse bekannt, das Bremer Landeskriminalamt (LKA) habe 2002 und 2005 über das Bundeskriminalamt (BKA) Informationen an US-amerikanische Bundesbehörden weitergeleitet. Im Anschluss an Äußerungen des Senators für Inneres und Sport in der Innendeputation, Nachfragen beim LKA hätten in einer ersten Einschätzung ergeben, dass es keine Zusammenarbeit mit amerikanischen Stellen gegeben hätte, habe ich mich nach Umfang und Art der übermittelten Daten und der legitimierenden Rechtsgrundlage erkundigt.

Mir wurde mitgeteilt, dass sich das LKA Bremen und die Staatsanwaltschaft Bremen nach Ausschöpfung aller Ermittlungsansätze um eine Vernehmung des wegen des Verdachts der Bildung einer kriminellen Vereinigung Beschuldigten bemüht haben. Hierfür haben sie sich am 14. Mai 2002, vor der Einleitung eines internationalen Rechtshilfeersuchens, an das BKA mit der Bitte gewandt, Kontakt zu amerikanischen Behörden aufzunehmen und verschiedene Fragen zu klären: Befindet sich

der Betroffene in amerikanischem Gewahrsam? Unter welchen Umständen erfolgte seine Festnahme? Wann ist mit seiner Entlassung zu rechnen? Können ggf. Ermittlungsergebnisse zur Verfügung gestellt werden? Stehen Hinderungsgründe rechtlicher und/oder tatsächlicher Art einer Vernehmung auf Guantanamo Bay durch den ermittelnden Staatsanwalt und einen Beamten des LKA entgegen?

Weiter wurde mir erklärt, im März 2005 habe eine in Bremen wohnhafte Person eine E-Mail an das FBI gerichtet und erklärt, der wahre Reisezweck des Murat Kurnaz sei die Beteiligung an einem heiligen Krieg gegen die Amerikaner gewesen. Das FBI habe sich daraufhin an das BKA mit der Bitte um Überprüfung sowie um Mitteilung ergänzender Informationen gewandt. Das BKA habe die Bitte an das LKA weitergeleitet. Das LKA habe den Absender der E-Mail und eine mit ihm befreundete Person befragt und sei gegenüber dem BKA zu dem Ergebnis gekommen, dass es sich vermutlich nicht um relevante Angaben handele. Das BKA habe dem Verbindungsbeamten des FBI darauf mitgeteilt, dass die in der E-Mail enthaltenen Angaben nicht bestätigt werden. In beiden Fällen seien Mitteilungen nur an das BKA, nicht unmittelbar an amerikanische Stellen erfolgt.

Rechtsgrundlage für die Anfrage wie für die Mitteilung von Ermittlungsergebnissen zur Vorbereitung eines Rechtshilfeersuchens ist § 3 Abs. 1 und 2 Bundeskriminalamtsgesetz (BKAG). Danach übernimmt das BKA als nationales Zentralbüro den Dienstverkehr mit öffentlichen Stellen anderer Länder. Somit lag bei den Datenweitergaben kein Verstoß gegen Datenschutzbestimmungen, etwa des BKAG oder des BremPolG, vor.

9.14 Speicherung von im Zentralruf der Polizei Bremen eingehenden Telefongesprächen

Ende 2005 unterrichtete mich die Polizei Bremen bei einem Besuch der Einsatzleitzentrale über Planungen, ab Januar 2006 die im Zentralruf der Polizei Bremen eingehenden Anrufe komplett, d. h. Sprach- und Verbindungsdaten, aufzuzeichnen.

Hiergegen habe ich im Dezember 2005 datenschutzrechtliche Bedenken geäußert. § 36 a Abs. 4 des Bremischen Polizeigesetzes (BremPolG) ermächtigt die Polizei Bremen, Anrufe über eine Notrufnummer aufzuzeichnen. Die Ermächtigung ist auf Notrufnummern begrenzt. Diese Notrufanschlüsse (110, 112) sind aufgrund ihrer Zweckbestimmung technisch besonders ausgestaltet. Sie besitzen u. a. eine Fangschaltung, um den Anschluss des Anrufers festzustellen, erlauben keine Rufnummernunterdrückung, können kostenfrei und bei Mobiltelefonen ohne Karte oder Kenntnis der PIN angerufen werden. Infolgedessen hat der Bundesgerichtshof festgehalten, dass andere Hauptanschlüsse der Polizei keine Notrufanschlüsse sind, auch wenn sie ebenfalls dem Anruf in Notfällen dienen (BGH, Beschluss vom 27. Januar 1986 – 3 StR 164/95). Ich bat daher um nähere Erläuterung, insbesondere der technischen Ausgestaltung des Zentralrufanschlusses und der Art der dort eingehenden Anrufe im Hinblick auf ihren Notrufcharakter.

Im März 2006 kam es zu einem Gespräch bei der Polizei Bremen, in dem ich meine Auffassung bekräftigte und insbesondere die Speicherung für drei Monate mit Blick auf die gesetzliche Speicherdauer von höchstens einem Monat (§ 36 a Abs. 1 Satz 2 BremPolG) für unzulässig erklärte.

Auf meine Nachfrage im August 2006 teilte die Polizei Bremen mir im September 2006 und auf Anfrage erneut im November 2006 mit, dass sie zwar an der Notwendigkeit der Speicherung aus polizeilicher Sicht festhalte, jedoch noch keine Maßnahmen zur Realisierung einer Aufzeichnung getroffen habe.

9.15 Unberechtigte Abrufe durch einen Feuerwehrbeamten bei der Meldebehörde

Ende Juni 2006 wandte sich eine Bürgerin an mich, weil ein Beamter der Feuerwehr Bremen zu ihrer Person sowie weiteren Familienangehörigen mehrfach Abfragen für private Zwecke aus dem Melderegister über seinen dienstlichen Computer durchgeführt habe.

Die Feuerwehr Bremen teilte mir zunächst mit, dass nach Untersuchung des Vorwurfs kein pflichtwidriges Verhalten des Beamten nachgewiesen werden könne, da eine Protokollierung, auf welche Personen und konkreten personenbezogenen Daten bei den Abrufen jeweils zugegriffen wird, auf Seiten der Feuerwehr Bremen nicht erfolge und der Beamte die Zugriffe bestreite. Daraufhin habe ich die Protokolle der

Meldebehörde des Stadtamtes überprüft, wo bei einem automatisierten Zugriff der Abruf protokolliert wird. Dabei konnte ich verschiedene Zugriffe des fraglichen Feuerwehrbeschäftigten feststellen. Die Protokolle übergab ich der Feuerwehr Bremen mit der Bitte, den dienstlichen Charakter der Zugriffe zu überprüfen und ggf. weitere Maßnahmen einzuleiten.

Die Feuerwehr Bremen hat nach Prüfung der Protokolle und Stellungnahme des Beamten ein Disziplinarverfahren eingeleitet.

9.16 Änderung des Bremischen Verfassungsschutzgesetzes

Mit Schreiben vom 13. November 2006 bin ich vom Senator für Inneres und Sport um Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Bremischen Verfassungsschutzgesetzes (BremVerfSchG) bis zum 17. November 2006 gebeten worden. Dabei sollten einige bis zum 11. Januar 2007 befristete Befugnisse des BremVerfSchG vom 28. Februar 2006 (Brem.GBl. 2006, S. 87) um weitere fünf Jahre bis zum Jahr 2012 verlängert werden.

Ich habe hierzu u. a. angemerkt, dass bislang die im Bremischen Verfassungsschutzgesetz vorgesehene Evaluation der Befugnisse nicht stattgefunden hat und auch nicht durch einen Verweis auf den Bericht der Bundesregierung zum Terrorismusbekämpfungsgesetz ersetzt werden kann. Auch bleibt die Regelung hinter der geplanten Bundesregelung zurück, die angesichts der Kritik an der fehlenden Unabhängigkeit und Wissenschaftlichkeit des Berichts nunmehr ausdrücklich eine Evaluation unter Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem deutschen Bundestag bestellt wird, vorsieht.

Daraufhin ist eine Verlängerung zunächst nur um drei Jahre bis 2010 vorgenommen worden. Dies erscheint ein genügend langer Zeitraum, um dann endlich eine Untersuchung der Eingriffsregelungen vorzunehmen.

9.17 Akkreditierungsverfahren der Fußball-Weltmeisterschaft 2006

Im 28. Jahresbericht (vgl. Ziff. 1.9 und 9.9) hatte ich über die Beteiligung des Landesamtes für Verfassungsschutz (LfV) und der Polizei Bremen im Rahmen des Akkreditierungsverfahrens zur Fußball-WM 2006 berichtet. Unabhängig von der fehlenden Rechtsgrundlage habe ich mich vor Ort über die Durchführung der Zuverlässigkeitsüberprüfung und über die Kriterien, die zur Abgabe eines negativen Votums führen, sowie über die Ausgestaltung des Rechtsschutzverfahrens informiert.

Zum Zeitpunkt meines Besuchs hatte das LfV acht Überprüfungen zu sieben Personen vorgenommen. Eine Person hatte erneut versucht, sich akkreditieren zu lassen und war zweimal aus denselben Gründen abgelehnt worden. Von den acht Anfragen kam es bei vier Personen zu Ablehnungen. In drei Fällen erfolgte die Zustimmung. Die Ablehnungen waren, unter Berücksichtigung des Kriterienkatalogs für die Überprüfung durch den Verfassungsschutz, in allen Fällen vertretbar und nicht zu beanstanden. Ich habe mich beim LfV davon überzeugt, dass jeweils aktuelle tatsächliche Anhaltspunkte für die Gefahr von Handlungen mit extremistischem Hintergrund oder für die Unterstützung bzw. Zugehörigkeit zu gewaltbereiten Bestrebungen vorlagen.

Das Landeskriminalamt Bremen hat insgesamt 789 Überprüfungen vorgenommen und davon in 671 Fällen seine Zustimmung und in 22 Fällen seine Ablehnung ausgesprochen. Auch hier waren die stichprobenartig von mir vorgenommenen Überprüfungen der Ablehnungen unter Berücksichtigung des Kriterienkatalogs vertretbar und nicht zu beanstanden.

9.18 Eingaben im Bereich des Verfassungsschutzes

Auch in diesem Jahr haben sich Bürger an mich gewandt, um ihre Betroffenenrechte gegenüber dem Landesamt für Verfassungsschutz (LfV) geltend zu machen.

So wandte sich in einem Fall ein Bürger an mich, dessen Einbürgerung im Ergebnis an Bedenken des LfV zu scheitern drohte, da er in extremistische Aktivitäten verstrickt sei. Ich habe daraufhin beim Senator für Inneres und Sport die zu dem Petenten vorliegenden personenbezogenen Angaben eingesehen und wegen Unklarheiten zur Identiät um eine erneute Einschätzung durch das LfV gebeten. In einer erneuten Einschätzung wurden die Bedenken zurückgezogen.

In einem anderen Fall bat ein Bürger um Unterstützung bei der Wahrnehmung seiner Betroffenenrechte. Nach Auskunft über die zu seiner Person beim LfV gespeicherten Daten bat er um Mitteilung, inwieweit falsche Angaben durch ihn richtig gestellt werden können.

9.19 Rahmendatenschutzkonzept und andere Verfahren beim Stadtamt Bremen

Im vergangenen Jahr hatte ich über das Fehlen des allgemeinen Rahmendatenschutzkonzeptes und verschiedener Fachdatenschutzkonzepte beim Stadtamt Bremen sowie eine Kick-Off-Veranstaltung im Februar 2006 zur Erstellung der Konzepte berichtet (vgl. 28. JB, Ziff. 9.15). Zunächst war bis Anfang April 2006 die Erstellung des Rahmendatenschutzkonzeptes und von vier Fachdatenschutzkonzepten für die Verfahren Waffenverwaltung, Einwohnermeldewesen, Gewerbeaufsicht und Kfz-Zulassungswesen vorgesehen.

Das Datenschutzkonzept für die Waffenverwaltung wurde mir im März 2006 vorgelegt. Hierzu habe ich im September 2006 Stellung genommen und verschiedene Änderungen am öffentlichen und nicht öffentlichen Teil des Datenschutzkonzeptes angeregt. So war die Darstellung der Lösch- und Sperrfristen unzureichend, auch bei den technischen und organisatorischen Maßnahmen bestanden Unzulänglichkeiten, insbesondere bei der Zutritts-, Zugriffs-, Weitergabe- und Eingabekontrolle. Bei verschiedenen Maßnahmen wurde auf das Rahmendatenschutzkonzept verwiesen, das noch nicht vorliegt und daher nicht in die Prüfung einbezogen werden konnte.

Darüber hinaus wurden mir im Sommer 2006 zu den Verfahren der Bearbeitung von Verkehrsordnungswidrigkeiten und zur Mobilen Datenerfassung Verkehrsüberwachung die Verfahrensbeschreibung und das Datenschutzkonzept übersandt. Die Datenschutzkonzepte für die Verfahren Einwohnermeldewesen, Gewerbeaufsicht und Kfz-Zulassungswesen wurden mir auf meine Aufforderung hin Ende Juni 2006 übersandt, ihre Prüfung ist noch nicht abgeschlossen.

Gleichzeitig wurde mir mitgeteilt, dass sich die Erstellung des Rahmendatenschutzkonzeptes aufgrund des im Stadtamt Bremen im Frühjahr über Monate geführten Streiks verzögert und erst im September 2006 mit der Erstellung begonnen werden könne. Der von April auf Ende des Jahres verschobene Zeitplan war auch Gegenstand der Beratungen im Rechtsausschuss. Im Ausschuss zugesagt wurde schließlich vom Stadtamt eine Erstellung bis zum Jahresende. Anfang 2007 wurde mir dann tatsächlich das Rahmendatenschutzkonzept zur Stellungnahme übersandt.

Für weitere IT-Fachanwendungen beim Stadtamt sind die Arbeiten am Datenschutzkonzept angelaufen oder sind für 2007 geplant, z. B. für das Verfahren zur Ausstellung von Führerscheinen.

9.20 Anmeldung zur Eheschließung per Internet

Ende Juli 2006 war der Startschuss für den Einsatz des neuen Datenverarbeitungsverfahrens xStA-Bürger bei den Standesämtern zur Vorbereitung von Eheschließungen. Ich wurde durch Nachfrage eines Journalisten darauf aufmerksam gemacht. Aus den im Internet veröffentlichen Unterlagen zu dem Verfahren war ersichtlich, dass die Verarbeitung der Daten von Heiratswilligen und weiterer Beteiligter, z. B. Kindern, Eltern, Trauzeugen vorgesehen ist und das Verfahren von einem Anbieter außerhalb Bremens im Wege der Auftragsdatenverarbeitung betrieben wird.

Ich habe daher Ende August 2006 die Standesämter angeschrieben und den Auftrag sowie das Datenschutzkonzept angefordert, die nach dem Bremischen Datenschutzgesetz (BremDSG) spätestens bei der Inbetriebnahme des Verfahrens fertiggestellt sein mussten. Im September 2006 habe ich an die Erledigung erinnert und auch den behördlichen Datenschutzbeauftragten des Stadtamtes Bremen informiert.

Ende November 2006 hat mir der behördliche Datenschutzbeauftragte des Stadtamtes Bremen nach einem Gespräch mit den Standesämtern die vorhandenen, aus datenschutzrechtlicher Sicht unzureichenden Unterlagen zur Beauftragung des Externen übersandt, diese beschränkten sich auf die Auftragsvergabe und die Vergütung, enthielten jedoch keine Datenschutzanweisungen an den Auftragnehmer. Auch die nach § 9 BremDSG vorzusehende Möglichkeit einer Datenschutzkontrolle beim Auftragnehmer fehlt ebenso wie das Datenschutzkonzept.

9.21 Datenverarbeitungsverfahren Fundinfo

In meinem 28. Jahresbericht (vgl. Ziff. 9.17) habe ich über die Einführung der Internet-Anwendung Fundinfo berichtet. Im Februar 2006 wurde mir der noch ausstehende, umfangreiche nicht öffentliche Teil und im Juli 2006 der öffentliche Teil des Datenschutzkonzepts übersandt. Ende November 2006 habe ich zum Datenschutzkonzept aus rechtlicher und technischer Sicht Stellung genommen. Soweit zu den technisch-organisatorischen Maßnahmen hierauf verwiesen wurde, erfolgte die Prüfung vorbehaltlich der Regelungen im noch ausstehenden Rahmendatenschutzkonzept (vgl. Ziffer 9.19 dieses Berichts). Änderungswünsche erfolgten zum Umfang der gespeicherten Daten, etwa der Bankverbindungsdaten des Eigentümers zur Einzugsermächtigung des Finderlohns sowie zum Umfang der beteiligten Einrichtungen und der Aufbewahrungs-, Sperr- und Löschfristen. Ferner ergaben sich Fragen der Auftragsdatenverarbeitung aufgrund des Betriebs durch einen Auftragnehmer mit Sitz außerhalb Bremens unter Einschaltung eines Rechenzentrums. Weitere Themen waren die Zugriffsberechtigung, das noch ausstehende Berechtigungskonzept, die Weitergabe- und Verfügbarkeitskontrolle im Hinblick auf die Netzinfrastruktur des Stadtamtes sowie Art und Umfang der Protokollierung.

Das Stadtamt Bremen hat die Klärung der von mir aufgeworfenen Fragen zugesagt. Zugleich wurde mitgeteilt, dass ein Zugriff der Polizei Bremen auf das Verfahren der Fundsachenverwaltung erfolgen soll, was verschiedene Änderungen des Datenschutzkonzeptes nach sich zieht. Insoweit steht ein konkretes Konzept noch aus.

9.22 Auskunftsrecht bei Behördenführungszeugnissen

Bewirbt sich jemand bei einem öffentlichen Arbeitgeber (Behörde), so wird auf Antrag der betroffenen Person in der Regel das Führungszeugnis unmittelbar an die Einstellungsbehörde übersandt (§ 30 Abs. 5 Satz 1 Bundeszentralregistergesetz [BZRG]), wobei die Einstellungsbehörde dem Bewerber auf Verlangen Einsicht in das Führungszeugnis zu gewähren hat. Die Betroffenen haben jedoch oft vorher schon ein Interesse das Führungszeugnis einzusehen, insbesondere, wenn Einträge vorhanden sind und um zu entscheiden, ob es der Einstellungsbehörde zugehen soll. Ein Bewerber kann daher für den Fall, dass das Führungszeugnis Einträge enthält, nach § 30 Abs. 5 Satz 3 BZRG verlangen, dass das Führungszeugnis zunächst an das dem Wohnort des Bewerbers nächstgelegene Amtsgericht zur Einsichtnahme durch ihn übersandt werden soll. Der Bewerber kann dann nach Einsichtnahme darüber entscheiden, ob das Führungszeugnis an die Einstellungsbehörde weitergeleitet oder vom Amtsgericht vernichtet werden soll.

Im September 2006 wandte sich eine Lehramtsbewerberin, die über die Meldebehörde ein Führungszeugnis zur Vorlage bei Behörden beantragen wollte, mit einem entsprechenden Anliegen an mich. Inwieweit dieses Verfahren der Meldebehörde bekannt war, ließ sich nicht feststellen. Im konkreten Fall war die Bewerberin jedoch über die Möglichkeit einer vorherigen Einsichtnahme nicht informiert worden. Ich habe die Betroffene über das Verfahren aufgeklärt und die Meldebehörde aufgefordert, in Zukunft über die Möglichkeit der Einsichtnahme beim Amtsgericht bei der Entgegennahme der Anträge zu informieren. Ein Antragsformular, in dem ein Verfahrenshinweis vermerkt werden könnte, gibt es nicht. Nach der Mitteilung der Meldebehörde Bremen werden Anträge auf Ausstellung eines Führungszeugnisses formlos angenommen und an das Bundeszentralregister weitergeleitet. Auch ein Online-Antragsverfahren wird derzeit nicht angeboten.

9.23 Online-Anmeldung von Kraftfahrzeugen durch Autohäuser

Aus der Presse konnte ich im August dieses Jahres entnehmen, dass Autohändler zukünftig die Daten für ihre Kfz-Anmeldungen online an die Zulassungsstelle übermitteln können. Es handelt sich hierbei um eine eGovernment-Anwendung, die hierfür einen ergänzenden Dienst zum Kfz-Zulassungsverfahren bereitstellt. Händler können über eine Eingabemaske die erforderlichen Daten erfassen und via Internet an die Zulassungsstelle übermitteln.

Es handelt sich hierbei nicht um die Möglichkeit der privaten Zulassung von Fahrzeugen bei Autohäusern. Lediglich die Datenerfassung wird auf Private verlagert, die diese dann in elektronischer Form an die Zulassungsstelle übermitteln. Da es sich hierbei überwiegend um Daten zu den Käufern handelt, die beim Fahrzeugkauf ohnehin von Händlern erfasst werden und die zugehörigen Fahrzeugdaten die-

sen bekannt sind, ging es vorrangig darum, eine sichere Übertragung der Daten zu gewährleisten.

Ich habe das Stadtamt aufgefordert, die Verfahrensbeschreibung (§ 8 Bremisches Datenschutzgesetz [BremDSG]) um diese Online-Komponente zu ergänzen. Darüber hinaus habe ich das Stadtamt darauf aufmerksam gemacht, dass die vorgesehene unverschlüsselte Weitergabe der Daten über das Internet, die nach § 7 Abs. 4 Satz 2 Nr. 4 BremDSG (Weitergabekontrolle) erforderliche Vertraulichkeit der Datenübermittlung nicht gewährt und daher unzulässig ist. Allerdings habe ich aufgrund der Zusage, dass für Ende 2006 die Datenübermittlung in sicherer Form (im OSCI-Format) vorgenommen werden wird, von einer Beanstandung des Verfahrens abgesehen. Mitte Januar 2007 war die Umstellung des Verfahrens nach Auskunft des Stadtamtes noch nicht initiiert. Als neuer Termin wurde der Frühsommer genannt.

Um die Weitergabekontrolle für den jetzt doch erheblich längeren Zeitraum zu gewährleisten, habe ich vom Stadtamt eine Verschlüsselung der Daten für die Übermittlung via Internet zum nächstmöglichen Zeitpunkt gefordert. Festzuhalten bleibt, dass vom Stadtamt gegen die nach § 27 Abs. 3 BremDSG bestehende Unterrichtungspflicht verstoßen wurde und das in der Presse gefeierte Modell für die Betroffenen zurzeit keinen ausreichenden Datenschutz sicherstellt.

9.24 Auskunft aus dem Fahrzeugregister an die GEZ

Ein Transportunternehmer beschwerte sich über einen Rundfunkgebührenbeauftragten von Radio Bremen, weil dieser eine Halter- und Fahrzeugabfrage bei der Kfz-Zulassungsstelle über seine Firmenfahrzeuge und das Fahrzeug seiner Ehefrau vorgenommen hatte.

Die öffentlich-rechtlichen Rundfunkanstalten und die von ihnen beauftragte GEZ sind regelmäßig an personenbezogenen Daten von Haltern von Kraftfahrzeugen interessiert. Da nahezu jedes Fahrzeug über ein Autoradio verfügt und die Meldequote insbesondere bei geschäftlich genutzten Fahrzeugen eher niedrig sei, versuchen die Rundfunkgebührenbeauftragten, Halterdaten bei den Fahrzeugregister führenden Zulassungsstellen zu bekommen. Als Rechtsgrundlage werden hierfür § 39 Abs. 3 Nr. 1 a Straßenverkehrsgesetz (StVG) oder § 35 Abs. 1 Nr. 3 StVG bemüht. Danach sind Halterauskünfte zur Verfolgung von Rechtsansprüchen in Höhe von jeweils mindestens 500 € oder zur Verfolgung von Ordnungswidrigkeiten zulässig.

Die GEZ bzw. die Rundfunkgebührenbeauftragten besitzen i. d. R. weder gegenüber dem Kraftfahrtbundesamt noch den örtlichen Zulassungsbehörden einen Auskunftsanspruch, weil eine Gebührenforderung von mindestens 500 € allenfalls in einem besonderen Ausnahmefall erreicht sein dürfte. Die angegebenen Rechtsgrundlagen erlauben keine verdachtslose Übermittlung von Daten, um im Anschluss zu prüfen, ob überhaupt eine Forderung oder eine Ordnungswidrigkeit wegen Bereithaltens von Rundfunkgeräten ohne Anmeldung besteht. Das bloße Bereithalten eines Rundfunkgeräts in einem Kraftfahrzeug ist nicht ausreichend für ein Auskunftsersuchen.

Auch im Beschwerdefall war es so. Die genannte Gebührenforderungsgrenze war nicht erreicht, eine Auskunft hätte nicht erteilt werden dürfen. Meine Auffassung habe ich dem Datenschutzbeauftragten von Radio Bremen sowie der Aufsichtsbehörde über die Kfz-Zulassungsstellen mitgeteilt.

10. Justiz

10.1 Anbindung der Amtsgerichte und Staatsanwaltschaft an das BZR

Beim Betrieb verschiedener EDV-Anwendungen wird die Staatsanwaltschaft Bremen durch die IuK-Stelle bei der Generalstaatsanwaltschaft Celle unterstützt. Grundlage hierfür ist eine Verwaltungsvereinbarung zwischen dem Senator für Justiz und Verfassung und der niedersächsischen Justizministerin aus dem Jahre 2005.

Im April 2006 habe ich das bei der Staatsanwaltschaft Bremen eingesetzte Verfahren zum elektronischen Datenaustausch mit dem Bundeszentralregister und Verkehrszentralregister geprüft. Bei der Prüfung des Verfahrens habe ich festgestellt, dass der Netzwerkverkehr nicht den Anforderungen an die Zugangskontrolle nach

dem Bremischen Datenschutzgesetz (BremDSG) entspricht. Darüber hinaus war permanent ein administrativer Zugriff auf die Daten der Staatsanwaltschaft Bremen seitens der Generalstaatsanwaltschaft Celle möglich, ohne dass die Vorgaben des BremDSG zur Auftragskontrolle gewahrt waren. Insbesondere waren die technischen und organisatorischen Maßnahmen und evtl. Unterauftragsverhältnisse nicht festgehalten und es war nicht sichergestellt, dass der Auftragnehmer die Bestimmungen des BremDSG beachtet und sich insoweit meiner Kontrolle unterwirft. Ich habe daher eine Anpassung der Verwaltungsvereinbarung gefordert und hierfür eine Formulierung vorgeschlagen.

10.2 Eröffnung des elektronischen Rechtsverkehrs

Im Berichtsjahr habe ich die vom Senator für Justiz und Verfassung (SfJuV) übersandten Unterlagen, u. a. die Verfahrensbeschreibung „Elektronischer Rechtsverkehr mit den Gerichten und Staatsanwaltschaften im Land Bremen“ datenschutzrechtlich bewertet. Die Verfahrensbeschreibung nebst der jeweils zugehörigen Dienstanweisung genügte im Wesentlichen den Anforderungen nach § 8 Bremisches Datenschutzgesetz. Es fiel aber auf, dass darin für die verschiedenen verantwortlichen Stellen unterschiedliche Löschfristen für im elektronischen Rechtsverkehr empfangene Dokumente und davon gefertigte Arbeitskopien festgelegt waren. Für zwei Dienststellen war der Umgang mit den Arbeitskopien nicht geregelt.

Mit Vertretern aus dem Justizressort habe ich besprochen, wie eine fristgerechte Löschung von Dokumenten aus dem elektronischen Rechtsverkehr zu erreichen ist. Es sollen klare Kommunikationswege definiert werden wie auch die Verantwortlichkeiten für die Löschung der Dokumente. Alle Dienststellen sollen entsprechende organisatorische Maßnahmen vornehmen, diese sollen in den jeweiligen Dienstanweisungen festgelegt werden. Der SfJuV hat zugesagt, die zur zentralen Verfahrensbeschreibung gehörende Musterdienstanweisung entsprechend anzupassen und bei allen beteiligten Stellen darauf hinzuwirken, dass die Änderungen umgesetzt werden. Ich habe daraufhin diesen Punkt gegenüber dem Rechtsausschuss der Bürgerschaft für erledigt erklärt.

11. Gesundheit und Krankenversicherung

11.1 Pilotprojekt zur Einführung der elektronischen Gesundheitskarte

Die Geschäftsstelle ARGE Bremer Initiative für Telematik im Gesundheitswesen (B.I.T.), Träger des Projekts zur Einführung der elektronischen Gesundheitskarte in der Testregion Bremen, schloss mit der Gematik einen Rahmenvertrag über die Zusammenarbeit, Unterstützung und Durchführung bezüglich der Testung der Telematikinfrastruktur. Die Gematik nimmt testregionenübergreifend die Aufgaben des Aufbaus der Telematikinfrastruktur, der Erstellung der technischen Vorgaben und der Sicherstellung der Test- und Zertifizierungsmaßnahmen wahr. Die Grundlage für den Testverlauf ist die „Rechtsverordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte vom 2. November 2005“, deren Anlagen die Spezifikationen für die elektronische Gesundheitskarte, den elektronischen Heilberufeausweis und die Kartenterminals sowie ein Test- und Migrationskonzept enthalten, wie auch den Zeitplan und die Festlegungen der Einzelheiten der Testung. Danach war geplant, im Frühjahr 2006 mit den Tests unter Einbeziehung von Versicherten in den Testregionen zu beginnen. Dieser Termin wurde im Laufe des Jahres jedoch mehrfach verschoben, bis Ende des Jahres bereits von einem Testbeginn im August 2007 die Rede war. Die genannte Rechtsverordnung ist im Oktober dieses Jahres dergestalt geändert worden, dass nunmehr auch Regelungen zur Testung der technischen Umsetzung der Wahrnehmung der Patientenrechte vorgesehen sind, was von Seiten der Datenschutzbeauftragten einhellig begrüßt wurde.

Im Vorfeld der Änderung der Rechtsverordnung bat mich das Gesundheitsressort um eine Stellungnahme zum Änderungsentwurf der Verordnung. Bei den zugehörigen technischen Beschreibungen handelte es sich um Dokumente von mehr als 1.000 Seiten. Dieser Bitte konnte ich aber wegen der knappen Personaldecke in meiner Dienststelle leider nicht entsprechen.

Eine verantwortliche Begleitung des Projektes konnte ich ohne zusätzliche personelle Unterstützung ohnehin nicht sicherstellen. Neben den Aufgaben vor Ort bestand Abstimmungsbedarf mit dem Bund und der Gematik über das Datenschutzkonzept zu den Anforderungen an die verwendeten Geräte inklusive der damit

verbundenen Zulassungsverfahren, sowie weitere Abstimmungsverfahren mit der B.I.T. und den Datenschutzbeauftragten der anderen beteiligten Länder, u. a. durch Gremienarbeit und Arbeitsgruppensitzungen. Ich wies daher das Gesundheitsressort und die B.I.T. frühzeitig darauf hin, dass ich aufgrund meiner personellen Situation lediglich die rechtlichen Fragestellungen begleiten könnte, für die technische Begleitung jedoch zwingend auf Unterstützung angewiesen sei. In einem Gesprächstermin mit der Handelskrankenkasse konnte ich immerhin erreichen, dass mir von dort eine Ansprechpartnerin für technische Fragen zur Verfügung stehen sollte. Nicht unerwähnt bleiben soll, dass ich bereits bei den Haushaltsberatungen deutlich gemacht hatte, dass ich ohne weitere Unterstützung meine gesetzlichen Aufgaben bei der Einführung der elektronischen Gesundheitskarte in dem erforderlichen Umfang nicht würde nachkommen können. Schließlich wurden im Oktober durch das Gesundheitsressort doch noch Überlegungen angestellt, wie eine Unterstützung gefunden werden könne. Zu einer Lösung der personellen Probleme ist es jedoch bis zum vorzeitigen Ende des Projektes dann nicht mehr gekommen.

Gleichwohl war ich das Jahr über bemüht, das irgendwie noch Leistbare zu erbringen, um die Option für eine datenschutzgerechte Durchführung des Pilotprojekts in Bremen so lange wie möglich noch offen zu halten. So überprüfte ich im Berichtsjahr den Entwurf für das „Gesamtkonzept Testverfahren in den Testregionen". Dieses Konzept enthielt Empfehlungen an die Projektträger in den Testregionen zur Organisation der Verfahren und zur Werbung der teilnehmenden Ärzte, Apotheken und Versicherten. Unter anderem wurde dort vorgeschlagen, nach der Auswahl der teilnehmenden Ärzte und Apotheken durch die Kassenärztlichen Vereinigungen oder die Krankenkassen anhand der dort vorhandenen Datenbestände auswerten zu lassen, welche Patienten die teilnehmenden Ärzte und Apotheken frequentierten und eine hohe Anzahl von Arztbesuchen und Verordnungen aufweisen. Diese Patienten sollten dann von den Krankenkassen kontaktiert werden. In einer anderen Variante sollte die Selektion durch die Ärzte stattfinden, die die Versicherten anhand von Kassenzugehörigkeit, Frequentierung und Verordnungshäufigkeit auswählen. Gegen diese Vorgehensweisen äußerte ich Bedenken, da die vorgeschlagenen Datennutzungen durch die Krankenkasse, die Ärzte und die Kassenärztlichen Vereinigungen nicht durch Rechtsgrundlagen gedeckt sind.

In Bremen war geplant, Tests mit 25 Arztpraxen, fünf Apotheken, einem Krankenhaus und 10.000 Versicherten durchzuführen. Zudem sollte Bremen eine bundesweit federführende Rolle bei der Weiterentwicklung und Testung der elektronischen Patientenakte wahrnehmen. Später wurde beschlossen, dass entgegen der ursprünglichen Planungen die freiwilligen Anwendungen (elektronischer Arztbrief, Medikamentendokumentation und die elektronische Patientenakte) zunächst nicht mehr im Testkonzept enthalten sein würden, die Tests sich also nur noch auf die im Gesetz genannten Pflichtanwendungen (Notfalldatensatz, elektronisches Rezept) erstrecken sollten. Auch das von der B.I.T. koordinierte Verfahren zur Werbung der Testteilnehmer in Bremen wurde in verschiedenen Varianten geplant und von mir jeweils datenschutzrechtlich beraten.

Anfang November ist das Pilotprojekt zur Einführung der elektronischen Gesundheitskarte in der Testregion Bremen schließlich gescheitert. Den Anstoß dazu gab die Kassenärztliche Vereinigung Bremen, die ihre Teilnahme an dem Projekt mit der Begründung aufkündigte, dass weder ein medizinischer noch ein wirtschaftlicher Nutzen in dem Projekt gesehen werde und die Einführung der elektronischen Gesundheitskarte nach einer aktuellen Kosten-Nutzen-Analyse in keinem Verhältnis zum tatsächlichen Ertrag stehe. Weiterhin wurde angeführt, dass der vorliegende Entwurf der Gesundheitsreform die Finanzgrundlagen der Kassenärztlichen Vereinigungen gefährde, weshalb eine Teilnahme an dem Projekt nicht mehr zu verantworten sei. Anschließend kündigten auch die Ärztekammer, die Psychotherapeutenkammer und der Apothekerverein ihre Teilnahme an dem Projekt auf. Die Ärztekammer begründete ihren Rückzug mit den erheblichen Verzögerungen im Zeitplan und Lücken in der technischen Umsetzung, wodurch der Nutzen in keinem Verhältnis zu den zu erwartenden Kosten stehe. Schließlich löste sich die B.I.T. auf, was dann zum Ausstieg Bremens aus dem Projekt zur Testung der elektronischen Gesundheitskarte führte.

11.2 Krankenkasse verlangt kompletten Einkommenssteuerbescheid

Ab Oktober 2005 erreichten mich zahlreiche Eingaben zu der Frage der Zulässigkeit der Anforderung des Einkommenssteuerbescheides für die Berechnung der Bei-

träge freiwillig versicherter Mitglieder durch eine Bremer Krankenkasse. Meine Rückfrage bei der Krankenkasse ergab, dass diese als einzige im Bundesgebiet zu diesem Zweck bisher noch keine Vorlage des Einkommenssteuerbescheides gefordert hatte, nunmehr jedoch aufgrund der Aufforderungen durch das Bundesversicherungsamt und die zuständige Aufsichtsbehörde beim Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales dazu verpflichtet sei. Die Aufforderung wurde gestützt auf § 206 Abs. 1 Sozialgesetzbuch (SGB) V, wonach der Versicherte der Krankenkasse auf Verlangen alle für die Feststellung der Versicherungs- und Beitragspflicht erforderlichen Auskünfte zu erteilen und Unterlagen, aus denen die Tatsachen oder die Änderung der Verhältnisse hervorgehen, vorzulegen hat. Nach der Satzung der Krankenkasse wird die wirtschaftliche Leistungsfähigkeit durch alle Einnahmen und Geldmittel bestimmt, die das Mitglied zum Lebensunterhalt verbraucht oder verbrauchen könnte. Seit der Einführung des Risikostrukturausgleichs, mit dem u. a. auch die beitragspflichtigen Einnahmen der Krankenkassen ausgeglichen werden, erkennen die Prüfdienste des Bundes und der Länder für freiwillig versicherte Selbstständige einen Betrag unterhalb der Beitragsbemessungsgrenze nur noch bei Vorlage amtlicher Unterlagen als Einkommensnachweise an. Einkommenserklärungen der Versicherten oder Nachweise des Steuerberaters werden dafür nicht mehr akzeptiert. Diese Praxis steht in Übereinstimmung mit der Rechtsprechung des Bundessozialgerichts (Urteile vom 26. September 1996 – 12 RK 18/95, 12 RK 46/95 und 12 RK 13/96), das ausführt, dass die Krankenkassen auf die Vorlage von Einkommenssteuerbescheiden angewiesen seien, da ihnen kein Instrumentarium zur Verfügung stehe, die Höhe der Bruttoeinnahmen der Versicherten aus selbstständiger Tätigkeit anderweitig festzustellen. Wegen des Steuergeheimnisses dürften sie nämlich keine Informationen über deren Einnahmen vom Finanzamt anfordern.

Einkommenssteuerbescheide enthalten jedoch eine Vielzahl von Daten, die für die Beitragsbemessung nicht erforderlich sind, z. B. Angaben über Ehepartner, wenn sie nicht bei einer anderen und privaten Krankenkasse versichert sind oder die Höhe der Steuern einschließlich etwaiger Erstattungen. Aus diesem Grunde bat ich die Krankenkasse, die Betroffenen in einem Merkblatt über die derzeitige Notwendigkeit der Vorlage von Einkommenssteuerbescheiden, die entsprechenden Rechtsvorschriften zur Auskunftspflicht (§ 206 i. V. m. §§ 240 ff. SGB V und die einschlägigen Regelungen in der Satzung) und die Möglichkeit des Schwärzens von nicht erforderlichen Daten zu unterrichten. Ebenso bat ich darum, in dem Merkblatt darauf hinzuweisen, dass auf Anfrage erklärt werde, welche Daten im individuellen Einzelfall nicht erforderlich sind sowie einen Hinweis aufzunehmen, dass bei Nichtvorlage des Bescheides der Höchstbetrag zu entrichten sei. Diesen Vorschlägen wurde durch die Krankenkasse entsprochen. Bedauerlich finde ich nach wie vor, dass nicht vorgesehen ist, dass die Finanzämter verpflichtet werden, auf Anforderung der Betroffenen aus dem ihnen vorliegenden Datensatz für die Vorlage bei einer Krankenkasse ein Ausdruckextrakt zu erzeugen, das nur die für das Antragsverfahren notwendigen Daten enthält. Das wäre zudem auch noch bürgerfreundlich.

11.3 Einladung bei Arbeitsunfähigkeit

Im April erhielt ich Kenntnis davon, dass eine Bremer Krankenkasse Versicherte, die eine bestimmte Zeit arbeitsunfähig krank geschrieben sind, schriftlich zu einem Informationsgespräch einlädt. Zu diesem Gespräch sollen die Versicherten einen ausgefüllten Fragebogen mit Datenerhebungen zur voraussichtlichen Dauer der Arbeitsunfähigkeit, zur durchgeführten medizinischen Behandlung und zum Inhalt der beruflichen Tätigkeit mitbringen. Ich wandte mich an den Datenschutzbeauftragten der Krankenkasse und fragte nach der Rechtsgrundlage und dem Zweck der Datenerhebungen, woraufhin dieser mir erläuterte, dass die Krankenkasse damit ihre in § 1 Sozialgesetzbuch (SGB) V normierte Pflicht zur Beratung der Versicherten wahrnehmen wolle. Ich wies ihn darauf hin, dass es für Datenerhebungen zu diesem Zweck keine gesetzliche Grundlage gebe und diese daher nur aufgrund einer Einwilligung der betroffenen Versicherten möglich sei. Ich half ihm bei der Formulierung einer nach § 67 b SGB X rechtmäßigen Einwilligungsklausel, die klarstellt, dass die Erteilung der Einwilligung auf der freien Entscheidung des Betroffenen beruht, den Betroffenen auf den Zweck der vorgesehenen Datenverarbeitung und -nutzung hinweist und klarstellt, dass eine Verweigerung der Einwilligung keine Auswirkungen auf das Versicherungsverhältnis zur Folge hat.

11.4 Datenerhebung der Steuerungsstelle Psychiatrie beim Martinshof

Die Steuerungsstelle Psychiatrie des Gesundheitsamtes ist fach- und ressourcenverantwortliche Stelle für den Bereich der Arbeit und Beschäftigung seelisch behinderter Menschen. Insoweit vertritt sie den Sozialhilfeträger im Fachausschuss der Werkstatt für behinderte Menschen (Martinshof). Der Fachausschuss veranlasst Überprüfungen und ggf. Veränderungen des Hilfeplans bzw. des Hilfebedarfs der dort betreuten Menschen. Für die Erfüllung dieser Aufgaben bat das Gesundheitsamt den Martinshof um die Übermittlung einer Vielzahl personenbezogener Daten über die Betreuten, u. a. Angaben über Diagnosen. Zum Umgang mit unklaren Diagnosen wie etwa, ob es sich um eine seelische oder geistige Behinderung handelt, gab es keine einheitliche Auffassung unter den Stellen.

Ich habe beiden Stellen auf Anfrage mitgeteilt, dass sowohl die Erhebung der oben genannten Daten durch die Steuerungsstelle Psychiatrie als auch die Übermittlung dieser Daten durch den Martinshof auf einer Rechtsgrundlage beruhen. Da die Steuerungsstelle Psychiatrie des Gesundheitsamtes als überörtlicher Sozialhilfeträger dem nach § 2 Abs. 1 Satz 2 Nr. 3 Werkstättenverordnung (WVO) zu bildenden Fachausschuss des Martinshofs angehört, nimmt sie entsprechende Aufgaben nach dem Sozialgesetzbuch (SGB) XII wahr. Demzufolge ist sie nach § 67 c Abs. 1 Satz 1 SGB X befugt, die zur Erfüllung dieser gesetzlichen Aufgaben erforderlichen personenbezogenen Daten der Betroffenen zu erheben. Demgegenüber ist der Martinshof eine Einrichtung nach § 75 SGB XII und § 136 SGB IX und damit nach § 69 Abs. 1 Nr. 1 SGB X befugt, der Steuerungsstelle Psychiatrie die für die Erfüllung der vorgenannten gesetzlichen Aufgaben erforderlichen personenbezogenen Daten zu übermitteln.

Ich habe mit beiden Stellen vereinbart, dass für die Wahrnehmung der Aufgaben der Steuerungsstelle Psychiatrie keine zusätzlichen Daten erhoben werden und ihr keine Einsicht in die Patientenunterlagen der Betroffenen gewährt wird. In den Fällen, in denen die Diagnose nicht eindeutig aus der Aktenlage erkennbar ist, wird vom Martinshof telefonisch in anonymisierter Form beim Gesundheitsamt aufgrund der Krankheitsgeschichte fachkundige Hilfe in Anspruch genommen. Sollte sich auf diesem Weg keine Diagnose ermitteln lassen, wird das Gesundheitsamt die betreffenden Personen begutachten lassen und im Zuge des Begutachtungsverfahrens nur nach wirksamer Einwilligung in die beim Martinshof befindlichen Krankenunterlagen Einsicht nehmen.

11.5 Aus der psychiatrischen Abteilung eines Bremer Krankenhauses

In der psychiatrischen Abteilung eines Bremer Krankenhauses waren im Flur Listen ausgehängt, die Namen der Patienten und ihrer Besucher einschließlich der Geschenke, die von diesen mitgebracht werden dürfen, enthielten. Dabei konnte nicht ausgeschlossen werden, dass Besucher und andere Personen den Inhalt dieser Listen zur Kenntnis nehmen, ohne dass dies erforderlich wäre. Außerdem gab es für die Patienten nur ein Telefon auf dem Flur, so dass es für diese nicht möglich war zu telefonieren, ohne dass andere Patienten, Ärzte und Pflegepersonen mithören konnten. Nach § 27 Abs. 6 Satz 2 in Verbindung mit § 28 Abs. 1 des Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (PsychKG) hat der Patient das Recht, im Rahmen einer allgemeinen Regelung ungestört Telefongespräche zu führen. Durch eine Kontaktaufnahme zur Klinikpflegeleitung konnte ich erreichen, dass die Liste mit dem Aushang über die Besuche nunmehr im Dienstzimmer der Station aufbewahrt wird. Um die Vertraulichkeit der Telefongespräche der Patienten zu gewährleisten, soll bis Ende des Jahres auf jeder Station eine Telefonzelle gebaut, in der Patienten mit einer entsprechenden Karte telefonieren können, so dass dem Personal die gewählten Nummern nicht bekannt werden und die Gespräche nicht mitgehört werden können. Durch diese Maßnahme soll auch sichergestellt werden, dass die Telefone nur von Patienten genutzt werden, denen eine freie Kontaktaufnahme nach außen erlaubt ist.

11.6 Mammographie-Screening

Von Bremen aus werden zurzeit alle Frauen in Bremen und Niedersachsen zwischen 50 und 69 Jahren zum Mammographie-Screening eingeladen. Seit Dezember 2005 wird von der „Zentralen Stelle für das Einladungswesen Mammographie-Screening“ des Gesundheitsamtes Bremen, die die Einladungen verschickt und die Teilnahme überwacht, die Software „MaSc“ eingesetzt. Um beurteilen zu können, ob den Anforderungen des Datenschutzes Rechnung getragen wird, hatte ich im

November 2005 eine Verfahrensbeschreibung und ein Sicherheitskonzept angefordert (vgl. 28. JB, Ziff. 11.3), welche mir im Juli 2006 vorgelegt worden sind. Da geplant ist, dass die Zentrale Stelle für das Einladungswesen beim Gesundheitsamt Bremen neben dem Versand der Einladungsschreiben für Bremen und Niedersachsen dies zukünftig auch für die Länder Hamburg und Sachsen-Anhalt wahrnimmt, drängen die Landesbeauftragten für den Datenschutz dieser Länder ebenfalls darauf, dass die Daten ihrer Bürger datenschutzgerecht verarbeitet werden und interessieren sich daher für meine datenschutzrechtliche Einschätzung.

Nach eingehender Prüfung der Verfahrensunterlagen habe ich um Nachbesserung einer Reihe von Punkten gebeten.

Da sich im Einladungsschreiben kein Hinweis auf die Möglichkeit zum Widerspruch gegen die Speicherung der Daten bei der Zentralen Stelle befand, bat ich um entsprechende Ergänzung der Unterlagen. Von Seiten der Zentralen Stelle des Gesundheitsamtes wurde hierzu ein Vorschlag unterbreitet, der nicht explizit auf die Widerspruchsmöglichkeit der Speicherung der Daten hinweist, denn es wurde befürchtet, dass der Anteil der am Screening teilnehmenden Frauen damit gesenkt werden würde. Im Einladungsschreiben sollen deshalb künftig die Frauen darauf hingewiesen werden, dass sie eine Mitteilung machen können, wenn sie nicht mehr angeschrieben werden wollen. Da aufgrund dieser Mitteilung die Identitätsdaten dieser Frauen nicht mehr verarbeitet werden, habe ich die Formulierung akzeptiert.

Ergänzungen im Datenschutzkonzept müssen auch noch hinsichtlich der Zugriffskontrolle (§ 7 Abs. 4 Nr. 3 Bremisches Datenschutzgesetz [BremDSG]) vorgenommen werden. Dies betrifft insbesondere den Schutz der Datenbank. Dabei müssen Fragen wie beispielsweise, wer direkten Zugriff auf die Datenbank hat, ob die Möglichkeit besteht, über eine interaktive Abfragesprache auf die Datenbank zuzugreifen, oder ob auf Betriebssystemebene auf die Dateien der Datenbank zugegriffen werden kann, beantwortet werden.

Für die Anonymisierung der Identitätsdaten aller Frauen ist die Bildung einer Screening-ID vorgesehen (vgl. 28. JB., Ziff. 11.3). Ich habe die Zentrale Stelle bereits im Dezember 2005 darauf hingewiesen, dass die Qualität der Nummer im Vergleich zu denen im Krebsregister verwendeten nicht dem Stand der Technik entspricht. Damals sagte die Zentrale Stelle zu, in den bundesweiten Gremien auf eine Änderung der Screening-ID hinzuwirken. Dies steht noch aus.

Weiterhin müssen im Konzept Festlegungen zur Gewährleistung der Eingabekontrolle erfolgen (§ 7 Abs. 4 Nr. 5 BremDSG). Es ist festzulegen, welche Ereignisse zu protokollieren und welche Informationen dabei zu erfassen sind. Darüber hinaus müssen Revisionsmechanismen beschrieben werden, beispielsweise, welche Benutzer unter welchen Rahmenbedingungen auf die protokollierten Informationen zugreifen dürfen und wann und nach welchen Kriterien diese Daten ausgewertet werden sollen. Auch Löschfristen sind zu definieren (§ 12 Abs. 4 BremDSG – enge Zweckbindung der Protokolldaten).

Die Zentrale Stelle des Gesundheitsamtes Bremen teilte mir mit, die erforderlichen Ergänzungen der Verfahrensunterlagen bis zum 31. Januar 2007 vorzunehmen und umzusetzen.

Ebenso bedeutsam wie eine bewertbare Dokumentation der technischen Datenschutzmaßnahmen ist die Aufklärung der Frauen hinsichtlich ihrer Datenschutzrechte. Immer wieder beklagten sich Frauen aus ganz persönlichen, z. T. sehr nachvollziehbaren Gründen bei mir, dass sie partout keine weitere Einladung erhalten möchten und fragten nach einer gangbaren Lösung. In diesem Jahr erreichten mich mehrere Eingaben von betroffenen Frauen, die bei der Zentralen Stelle telefonisch darum gebeten hatten, aus der Liste der einzuladenden Frauen gelöscht zu werden, worauf sie einen Anspruch haben, weil die Teilnahme freiwillig ist, von dort jedoch die Information erhalten hatten, dass dies technisch nicht möglich sei. Die Frauen wurden stattdessen an das Meldeamt verwiesen, um dort eine Übermittlungssperre für den Zweck des Mammographie-Screenings zu erwirken, obwohl es im Meldegesetz keine Rechtsgrundlage für die angeratene Übermittlungssperre gibt. Schließlich bekam ich von der Zentralen Stelle die Auskunft, dass nun sichergestellt sei, dass keine personenbezogenen Daten von Frauen, die der Speicherung widersprochen haben, in die Einladungsdatenbank übernommen würden und diese Frauen nach zwei Jahren keine erneute Einladung bekämen, solange sich ihr Meldedatensatz nicht ändere.

12. Arbeit und Soziales

12.1 Beschwerden über die Bremer Arbeitsgemeinschaft für Integration und Soziales

Im Berichtsjahr ist die Zahl der Eingaben und Beschwerden von Leistungsempfängern des Arbeitslosengeldes 2 (ALG II), die bei mir eingelegt wurden, eskaliert. Aus der Vielzahl sollen an dieser Stelle einige exemplarisch herausgegriffen werden:

Die Mutter eines leistungsempfangenden Schülers beklagte sich darüber, dass die Bremer Arbeitsgemeinschaft für Integration und Soziales (BAgIS) von ihrem Sohn die Vorlage eines Schulzeugnisses gefordert und für den Fall der Weigerung mit der Einstellung der Leistungen gedroht hatte. Auf ihre Nachfrage bei der BAgIS habe sie die Auskunft bekommen, diese Angelegenheit sei datenschutzrechtlich geklärt.

Mit wem die BAgIS die Anforderung von Schulzeugnissen abgeklärt hatte, ließ sich nicht feststellen. Gleichwohl wird die Praxis der Anforderung von Schulzeugnissen derzeit von allen Geschäftsstellen der BAgIS betrieben. Mit Nachdruck treten diese für die Einsicht in Schulzeugnisse ein, die zur Wahrnehmung der Integrationsbemühungen benötigt würden.

Da nicht nachgewiesen werden konnte, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), in dessen Zuständigkeit ein zugehöriger Leitfaden der Bundesagentur für Arbeit fällt, an dieser Frage beteiligt wurde, wird die BAgIS die derzeitige Praxis der Anforderung von Schulzeugnissen bis zu einer Klärung aussetzen. Ich sagte im Gegenzug zu, diese Angelegenheit in Abstimmung mit den Datenschutzbeauftragten des Bundes und der Länder zu klären.

Eine Kundin der BAgIS – Geschäftsstelle Nord – wandte sich an mich und berichtete, dass sie für ihren Erstantrag auf die Gewährung von Leistungen nach dem Sozialgesetzbuch (SGB) II bereits bei der Anmeldung Sozialdaten habe offenbaren müssen. So habe man sie gefragt, wovon sie bisher gelebt habe. Die Tür zum Anmeldezimmer, in dem zwei Kunden gleichzeitig bedient würden, stehe stets offen. Davor sei ein Stuhl für Wartende platziert, von dem aus jedes Gespräch bei der Anmeldung mitgehört werden könne. Sie habe daher z. B. mitbekommen, dass andere Kunden die Frage beantworten mussten, warum ein von ihnen eröffnetes Lokal, dessen Name genannt wurde, nicht „gelaufen“ sei. Auf ihre Frage hin gegenüber der Sachbearbeiterin, ob sie die ihr gestellten sensiblen Fragen nicht in einem separaten Raum beantworten könne, habe man ihr geantwortet, dass dies nicht möglich sei. Die Antragsaufnahme selbst würde in Büros mit zwei Sachbearbeitern mit Publikumsverkehr bearbeitet, deren Schreibtische in Hörweite nebeneinander stünden, wodurch die für den Antrag erhobenen Sozialdaten auch dem Sachbearbeiter und seinen Kunden am Schreibtisch nebenan zur Kenntnis gelangen würden. Dabei habe die Kundin beispielsweise mitbekommen, dass die Kundin, die namentlich angesprochen wurde, am Nebentisch dazu aufgefordert wurde, sich eine billigere Wohnung zu nehmen.

Ich gab der BAgIS Nord die Schilderungen der Kundin zur Kenntnis, wobei ich deren Wunsch berücksichtigte, ihren Namen nicht zu nennen, da sie ansonsten Nachteile in der Behandlung durch die BAgIS befürchtete. Zudem wies ich darauf hin, dass Sozialdaten durch das Sozialgeheimnis in § 35 Abs. 1 Satz 2 SGB I geschützt sind, wonach die Verpflichtung besteht, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind und nur an diese weitergegeben werden. Nachdem zunächst keine Reaktion der BAgIS Nord erfolgte, wurde mir auf Nachfrage mitgeteilt, dass mein Schreiben wohl verlorengegangen sei. Schließlich bekam ich zur Antwort, dass ohne Nennung des Namens der Kundin keine Stellungnahme zur Beschwerde abgegeben werden könne. Man versicherte mir jedoch, dass der Ablauf der Erstantragsaufnahme durch die Sachbearbeiter in den doppelt besetzten Büros so geregelt sei, dass immer nur ein Klient bedient werde, während sich der Sachbearbeiter am Nebentisch mit der Eingabe der Daten in das System befasse. Es könne zwar passieren, dass Kunden Unterlagen nachreichten und dafür ohne Aufforderung die Büros betreten und Fragen stellen würden. Für Neuanträge würden jeweils halbstündig Termine vergeben, so dass es unmöglich sei, zwei Kunden gleichzeitig zu bedienen. Der Stuhl vor dem Anmeldezimmer sei eine zusätzliche Sitzgelegenheit aufgrund des geringen Platzangebotes im Wartebereich.

Da die beiden Schilderungen sich deutlich widersprachen, war es notwendig, sich selbst ein Bild von den Gegebenheiten vor Ort zu machen. Dort befand sich direkt

gegenüber der Treppe ein Schild in DIN-A4-Größe mit der Aufschrift: „Datenschutz – Teilen Sie bitte mit, wenn Ihr Anliegen in einem separaten Büro besprochen werden soll oder Sie nicht namentlich aufgerufen werden wollen." Als Wartebereich diente ein ausreichend großer Flur, in dem sich die Kunden Wartemarken zogen, deren Nummern der Reihe nach in einer Anzeigentafel aufleuchteten und zum Betreten eines der beiden Anmeldezimmer aufforderten. Die Türen der beiden Anmeldezimmer waren geschlossen, so dass im Wartebereich keine Gespräche mitgehört werden konnten. Ich informierte die Kundin telefonisch über meine Beobachtungen, die sich über die verbesserte Situation sehr erfreut zeigte.

Eine andere Kundin der BAgIS – Geschäftsstelle Nord – wandte sich an mich, weil ihr die Einsicht in ein durch den psychologischen Dienst der Agentur für Arbeit im Auftrag der BAgIS erstelltes Gutachten zu ihrer Erwerbsfähigkeit sowohl von der BAgIS als auch vom psychologischen Dienst versagt worden war. Zudem war sie von der BAgIS unter Hinweis auf ihre Mitwirkungspflicht zum Ausfüllen eines Fragebogens über ihren Gesundheitszustand und zur Entbindung ihrer Ärzte von der Schweigepflicht gedrängt worden. Da sie dem nicht nachkommen wollte, wurden ihre Leistungen um 30 % gekürzt. Durch meine Intervention wurde die Forderung nach der Schweigepflichtentbindung durch die BAgIS fallengelassen. Stattdessen füllte die Kundin den Fragebogen aus, woraufhin die Kürzung ihrer Leistungen wieder rückgängig gemacht wurde. Zudem wurde ihr zwar die Einsicht in das Gutachten gestattet, jedoch die Anfertigung von Kopien verwehrt. Ich wandte mich erneut an die BAgIS und den psychologischen Dienst der Agentur für Arbeit und wies darauf hin, dass die Kundin nach § 25 Abs. 5 SGB X ebenfalls einen Anspruch auf Anfertigung von Kopien des Gutachtens hat; dies wurde ihr dann auch gewährt.

Im August erhielt ich durch eine Beschwerde Kenntnis davon, dass der Briefkasten der BAgIS – Geschäftsstelle West – derart beschädigt war, dass die dort eingeworfenen Briefe von außen leicht wieder herausgenommen werden konnten. Ein Kunde wollte daher seinen Brief beim Pförtner abgeben, den dieser jedoch nicht annehmen wollte. Ich wies die BAgIS darauf hin, dass die Verpflichtung zur Wahrung des Sozialgeheimnisses nach § 35 Abs. 1 Satz 2 SGB I umfasst, dass auch innerhalb des Leistungsträgers sichergestellt werde, dass Sozialdaten nur Befugten zugänglich gemacht würden und bat darum, unverzüglich Maßnahmen zu ergreifen, die einen gesicherten Postempfang ermöglichen.

Ich bekam zur Antwort, dass das Problem bereits erkannt worden sei und an einer Lösung gearbeitet werde – eine schöne Formulierung. Der Briefkasten sei durch Einsatz schwerer Werkzeuge mehrfach beschädigt worden, weshalb nach einer Lösung gesucht werde, die solchen Angriffen in Zukunft standhalte. Vom Amt für Soziale Dienste (AfSD) werde die Installation eines Einwurfschlitzes im Mauerwerk geprüft, wobei es jedoch voraussichtlich Probleme mit den Vorschriften des Denkmalschutzes geben werde. Ersatzweise solle ein absolut sicherer freistehender Briefkasten angebracht werden. Ich begrüßte den Willen der BAgIS, sich um eine nachhaltige Lösung zu bemühen, äußerte jedoch die Befürchtung, dass die endgültige Lösung des Briefkastenproblems wohl noch etwas Zeit in Anspruch nehmen würde und bat eindringlich darum, eine Übergangslösung zu finden, die sicherstellt, dass die bei der BAgIS eingehende Post nicht von Unbefugten zur Kenntnis genommen werden kann. Ich schlug daher vor, den beschädigten Briefkasten abzumontieren und ein Schild anzubringen, das darauf hinweist, dass die Post übergangsweise zu den Öffnungszeiten in einem bestimmten Raum im Gebäude abgegeben werden könne. Leider konnte diese Lösung aus mir nicht bekannten Gründen nicht umgesetzt werden. Stattdessen wandte sich das AfSD jetzt selbst an mich und fragte nach den besonderen Anforderungen des Datenschutzes für einen Briefkasten. Ich formulierte die allgemeinen technischen Anforderungen und unternahm einen weiteren Versuch, mich für eine sichere Übergangslösung einzusetzen, womit ich jedoch erneut scheiterte. Nach mehr als zwei Monaten erhielt ich dann schließlich vom AfSD die Auskunft, dass ein sicherer Außenbriefkasten montiert werde.

In einem anderen Fall wurde ich um Bewertung eines Vorhabens gebeten, wonach bei jugendlichen Leistungsempfängern, die eine Schule besuchen, eine besondere Schulbescheinigung verwendet werden soll, aus der hervorgeht, ob ein regelmäßiger Schulbesuch vorliegt. Hintergrund ist der, dass nach § 7 SGB II Jugendliche ab dem 15. Lebensjahr bei Vorliegen der entsprechenden Voraussetzungen selbst zum Bezug von ALG II anspruchsberechtigt sind. Also gilt auch für sie der Grundsatz des Forderns in § 2 SGB II, wonach jeder Leistungsempfänger alle Möglichkeiten zur Beendigung oder Verringerung der Hilfebedürftigkeit auszuschöpfen hat,

insbesondere durch eine Arbeitsaufnahme, es sei denn, dass dieser ein wichtiger Grund entgegensteht (§ 10 Abs. 1 Nr. 5 SGB II). Ein regelmäßiger Schulbesuch ist als ein solcher wichtiger Grund zu bewerten. Aus der derzeit verwendeten Schulbescheinigung geht jedoch nicht hervor, ob der Jugendliche die Schule regelmäßig besucht. Werde die Schule nicht regelmäßig besucht, würde die BAgIS mit den Jugendlichen und ihren Erziehungsberechtigten eine Eingliederungsvereinbarung über den Schulbesuch nach § 15 SGB II abschließen.

Ich unterstützte die BAgIS daher bei der Formulierung eines eigenen Formulars, auf dem sich zwei alternativ anzukreuzende Felder „Schulbesuch regelmäßig“ oder „mehr als 14 unentschuldigte Fehltage im letzten Schuljahr“ befinden. Dieses Formular soll der jugendliche Antragsteller in seiner Schule ausfüllen lassen, so dass keine Datenübermittlung von der Schule zur BAgIS erforderlich ist. Der Vordruck enthält keinen Briefkopf, so dass daraus nicht erkennbar ist, dass es sich um einen Vordruck der BAgIS handelt. Realistischerweise muss jedoch trotzdem davon ausgegangen werden, dass sich auf Dauer nicht verhindern lassen wird, dass die unterzeichnende Person dadurch den Jugendlichen als Bezieher von ALG II erkennen wird. Die neue Schulbescheinigung befindet sich derzeit noch im Verfahren der Abstimmung vom Senator für Bildung und Wissenschaft und wird noch nicht verwendet.

Ein Kunde der BAgIS – Geschäftsstelle Süd – hatte einen Antrag auf ALG II gestellt, dem für den Zeitraum von Februar bis Mai 2006 stattgegeben wurde. Aufgrund einer krankheitsbedingten Erwerbsunfähigkeit ist es jedoch nicht zur Auszahlung von Leistungen gekommen. Dessen ungeachtet teilte die BAgIS ihm mit, dass beim Bundeszentralamt für Steuern ein automatisierter Datenabgleich für das Jahr 2004 durchgeführt worden sei; der Abgleich bezog sich also auf einen Zeitraum zwei Jahre vor der Antragstellung. Ich wandte mich an die BAgIS mit dem Hinweis, dass der automatisierte Datenabgleich nach § 52 Abs. 1 Nr. 3 SGB II nur bei Personen durchgeführt wird, die Leistungen nach dem SGB II beziehen und bat daher um Mitteilung der Rechtsgrundlage für diesen Datenabgleich. Weiterhin bat ich um Erklärung, warum ein Datenabgleich für das Jahr 2004 erforderlich war, obwohl die Leistungen für 2006 bewilligt worden waren. Es dürfen nur die Daten erhoben werden, die zur Überprüfung des bei der Sozialleistung zu berücksichtigenden Einkommens und Vermögens erforderlich sind. Meine Anfrage vom Oktober wurde im Berichtsjahr nicht mehr beantwortet.

Eine Kundin der BAgIS – Geschäftsstelle Süd – berichtete mir, dass sie von der BAgIS einen Leistungsbescheid erhalten habe, dessen dritte Seite Name, Geburtsdatum und Kundennummer einer anderen Person enthielt, so dass sie erkennen konnte, dass es sich bei dieser Person um einen Empfänger von ALG II handelt. Leider ließ sich dieser Fehler nicht weiter aufklären, weil die Kundin die Unterlagen der fremden Person, die sie unberechtigterweise erhalten hatte, aus Angst, sich strafbar zu machen, sofort vernichtet hatte.

12.2 Änderung des Bundesvertriebenengesetzes

Ich habe gegenüber dem Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales zu dem vorgenannten Gesetzentwurf (Stand: 30. Juni 2006) Stellung genommen, mit dem die Ausschlussgründe erweitert und modifiziert sowie eine Abfrage bei den Sicherheitsbehörden in Anlehnung an die Regelungen des Aufenthaltsgesetzes und des Staatsangehörigkeitsgesetzes eingeführt werden sollen.

Dabei habe ich u. a. Zweifel geäußert, ob die hierfür im Entwurf vorgesehenen Regelanfragen bei dem Bundesnachrichtendienst, dem Bundesamt für Verfassungsschutz, dem Militärischen Abschirmdienst, dem Bundeskriminalamt und dem Zollkriminalamt und die Erweiterung der Ausschlussgründe mit dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit vereinbar sind. Die Regelanfragen würden alle betroffenen Personen unter einen Generalverdacht stellen. Auch der darin vorgeschriebene Vergleich von Ausschlussgründen zur Einbürgerung mit der Verteilung einer im Ausland begangenen Tat mit einer Begehung im Inland ist problematisch. Es erscheint fraglich, inwieweit Sachbearbeiter in der Lage sein werden, eine etwa in den ehemaligen Gebieten der Sowjetunion begangene Tat mit deutschen Straftaten zu vergleichen, insbesondere, wenn die Tatbegehung im Aussiedlungsgebiet unterschiedlichen rechtlichen Voraussetzungen unterliegt. Fraglich bleibt auch, wie der subjektive Tatbestand ermittelt werden soll. Problematisch wäre auch der Vergleich von Verbrechenstatbeständen, wie Friedensverrat, Hoch-

verrat oder Gefährdung des demokratischen Rechtsstaats, da entsprechende Taten in Aussiedlungsgebieten ohne rechtsstaatliche Tradition oft extensiv und/oder politisch beeinflusst geahndet werden.

Die senatorische Dienststelle hat meine Bedenken in ihrer Stellungnahme aufgenommen und mich regelmäßig über das weitere Gesetzgebungsverfahren unterrichtet. Der dem Bundesrat seit Anfang November 2006 vorliegende aktualisierte Entwurf enthält keine wesentlichen Änderungen.

12.3 Prüfung der Datenverarbeitung im Dienstleistungszentrum Grünhöfe

Im Oktober dieses Jahres habe ich die Netzinfrastruktur des Dienstleistungszentrums Grünhöfe in Bremerhaven geprüft. Das Dienstleistungszentrum wird von dem Arbeitsförderungszentrum des Landes Bremen GmbH, der Arbeiterwohlfahrt Kreisverband Bremerhaven e. V., dem Amt für Jugend und Familie der Stadt Bremerhaven, dem faden e. V., dem Kulturamt Bremerhaven und der Wirtschafts- und Sozialakademie der Arbeitnehmerkammer Bremen gGmbH gemeinsam betrieben. Die einzelnen Träger arbeiten organisatorisch unabhängig voneinander. Informationstechnisch benutzen alle Träger zur Erfüllung ihrer Aufgaben eine gemeinsame Netzinfrastruktur, die u. a. auch die Internetanbindung und die Abwicklung des E-Mail-Verkehrs ermöglicht. Diese Infrastruktur wird vom Amt für Jugend und Familie der Stadt Bremerhaven administriert.

Aufgrund der Angebotsstruktur einzelner Träger werden sehr sensible personenbezogene Daten verarbeitet. Das hierfür erforderliche Datenschutzniveau muss deshalb sowohl seitens der Träger als auch durch die gemeinsam genutzte Netzinfrastruktur gewährleistet werden. Inhalt meiner Prüfung war deshalb die technische Umsetzung der erforderlichen Abschottung der Daten der einzelnen Träger voneinander und die Absicherung des Gesamtnetzes.

Die Ergebnisse dieser Prüfung waren: Im Bereich der Protokollierung, Administration und Netzstruktur fehlen noch einzelne Dokumentationen. Ebenso muss noch ein schriftlicher Auftrag der Trägergemeinschaft an das Amt für Jugend und Familie Bremerhaven zur Administration der zentralen Netzstruktur (vgl. § 9 Bremisches Datenschutzgesetz [BremDSG]) erfolgen. In den von mir geprüften Bereichen Grundstruktur und Benutzerorganisation, Verzeichnis- und Netzinfrastruktur, Abschottung gegenüber dem Internet und Administration waren die technischen Maßnahmen grundsätzlich geeignet, die hierfür jeweils geltenden Anforderungen angemessen zu erfüllen.

Insgesamt handelt es sich um ein gutes Beispiel, Synergieeffekte durch die Nutzung einer gemeinsamen Infrastruktur unter Integration technischer Datenschutzmaßnahmen zu nutzen.

13. Bildung und Wissenschaft

13.1 Novellierung des Bremischen Schuldatenschutzgesetzes

Vor drei Jahren begann der Senator für Bildung und Wissenschaft mit seinen Arbeiten an der Novellierung des Bremischen Schuldatenschutzgesetzes (BremSchulDSG [vgl. 27. JB, Ziff. 10.3 und 28. JB, Ziff. 13.3]). Verzögerungen ergaben sich in der letzten Phase durch Intervention des Innenressorts. Inzwischen konnte Einvernehmen hergestellt werden. Der aktuelle Gesetzentwurf ist im Dezember 2006 in der Bildungsdeputation beschlossen worden. Der Gesetzentwurf wurde noch im Dezember 2006 in die Bürgerschaft (Landtag) eingebracht, die erste Lesung findet voraussichtlich im Januar 2007 statt.

Die Novellierung des aus dem Jahre 1987 stammenden BremSchulDSG war überfällig, weil sich die Informations- und Kommunikationstechnologie innerhalb der letzten 20 Jahre auch im Schulbereich rasant entwickelt hat. Neben den jahrelangen Erfahrungen in der Anwendung dieses Gesetzes war aufgrund der EU-Datenschutz-Richtlinie aus dem Jahre 1995 eine Anpassung des Bremischen Datenschutzgesetzes (BremDSG) und damit auch des BremSchulDSG notwendig. Folgende wesentliche Neuerungen prägen nunmehr das BremSchulDSG:

– Geltung des Gesetzes auch für Privatschulen: Das BremSchulDSG soll nunmehr auch für die Ersatzschulen und anerkannten Ergänzungsschulen (Privatschulen) gelten, weil Schülerdaten dort in der gleichen Intensität wie in öffentlichen Schulen

verarbeitet werden und diese Schulen auch der Aufsicht des Senators für Bildung und Wissenschaft unterliegen (§ 1 BremSchulDSG).

– Zulässigkeitsregelungen im Gesetz und Datenkatalog in der Rechtsverordnung: In § 2 BremSchulDSG ist materiell-rechtlich geregelt, zu welchen Zwecken Schüler- und Elterndaten verarbeitet werden dürfen. Hierbei ist auch festgelegt worden, dass die Daten auch zum Übergang vom Kindergarten- in den Schulbereich verarbeitet werden dürfen. Wegen des erhöhten Schutzbedarfs besonderer Arten von Daten in Schulen werden diese Daten ausdrücklich im Gesetz aufgeführt (Religionszugehörigkeit, Staatsangehörigkeit, Aussiedlereigenschaft, Muttersprache und Gesundheit). Alle übrigen personenbezogenen Schüler- und Elterndaten werden in einer Rechtsverordnung – unter Angabe der jeweiligen Zwecke – aufgeführt. Mit dieser Rechtskonstruktion will das Bildungsressort flexibler auf eine evtl. Ergänzung bzw. Änderung des zur jeweiligen Aufgabenerfüllung erforderlichen Datenkatalogs reagieren.

– Datenverarbeitung durch Lehrkräfte außerhalb der Schule: Heutzutage verfügt praktisch jede Lehrkraft über einen Privat-PC zu Hause, so dass in § 3 BremSchulDSG praxis- und datenschutzkonform festgelegt worden ist, dass Lehrkräfte Schülerdaten am häuslichen PC verarbeiten dürfen, wenn sie sich schriftlich zur Einhaltung der Datenschutzvorschriften verpflichten. Außerdem müssen sie sich mit häuslichen Kontrollmöglichkeiten der schulbezogenen Datenverarbeitung einverstanden erklären.

– Datenübermittlung an andere öffentliche Stellen: Neben den allgemeinen Voraussetzungen zur Datenübermittlung an andere öffentliche Stellen bzw. Behörden ist in § 8 BremSchulDSG ausdrücklich festgelegt worden, dass bei einer Entscheidung über eine derartige Datenübermittlung der Erziehungs- und Bildungsauftrag der Schule sowie das Vertrauensverhältnis zwischen Schülerinnen und Schülern und der Schule zu berücksichtigen sind. Die Datenübermittlung darf nur durch die Schulleitung erfolgen.

– Wissenschaftliche Forschung und Untersuchungen: Während grundsätzlich bei derartigen Vorhaben die Einwilligung der Schüler und – abhängig vom Alter bzw. Reifegrad der Schülerinnen und Schüler – ihrer Erziehungsberechtigten erforderlich ist, kann auf die Einwilligung verzichtet werden, wenn derartige Vorhaben unter Verwendung pseudonymisierter Daten erreicht werden kann (§ 13 BremSchulDSG). Hierbei müssen im Gesetz festgelegte Voraussetzungen erfüllt sein.

13.2 Bundeszentrale Datei über Schüler und Lehrer

Die Kultusministerkonferenz (KMK) hat vor ca. drei Jahren vereinbart, die bisherige Schulstatistik auf Individualdaten umzustellen und hierbei einen bundeseinheitlichen Kerndatensatz zu entwickeln. Dieses Vorhaben sei aufgrund der empirischen Wende in der Bildungspolitik und Pädagogik sowie der Beteiligung an internationalen Vergleichsuntersuchungen wie z. B. Pisa erforderlich, auch wenn die Belastbarkeit der Ergebnisse dieser Vergleiche von Fachleuten in Frage gestellt werden. Die Daten sollen der laufenden Information über relevante gesellschaftliche und strukturelle Entwicklungen im Bildungsbereich (Bildungsbericht und amtliche Statistik) dienen und als Basis für die Berechnung von Prognosen und Modellrechnungen, für die Entwicklung politischer und administrativer Maßnahmen sowie als Informationsquelle über den Stand der Zielerreichung (z. B. EU-Benchmarks) und zur Überwachung der Wirksamkeit bildungspolitischer Maßnahmen dienen.

Der Kerndatensatz solle über Schüler- und Lehrer-Identitäts-Nummern (ID) nur pseudonymisierte Daten enthalten mit dem Ziel, die Daten möglichst vom Kindergarten bis zum Abitur, Hochschulabschluss, Berufseinstieg und dem ersten Karrieresprung zu erfassen, wobei es unter den verschiedenen Bundesländern scheinbar noch unterschiedliche Lesarten der Beschlüsse gibt.

Schon frühzeitig habe ich den Senator für Bildung und Wissenschaft auf verschiedene Datenschutzbelange hingewiesen, die bei der Verfolgung eines solchen Ziels berücksichtigt werden müssen. Notwendig hierfür wäre eine verfassungskonforme Rechtsgrundlage und bei einer zentralen Zusammenführung der Daten könne hierfür ggf. ein entsprechender Staatsvertrag der Länder erforderlich sein. Auch sei festzulegen, ob die Aufgabe von bildungspolitischen Stellen oder Statistikämtern ausgeführt werden solle.

Allerdings steht das ganze Projekt unter dem Vorbehalt, dass der Aufbau eines solchen schülerbeziehbaren Datensatzes erforderlich ist. Eine Erhebung der Daten bei allen Schülern kommt allenfalls dann in Betracht, wenn nachgewiesen wird, dass eine intelligente Teilerhebung (vergleichbar einem Mikrozensus) nicht zum Ziel führen würde und dies nicht nur aus Kostengründen. Allerdings lassen die bisher aus Gremien der KMK genannten Gründe für den Kerndatensatz noch keine präzise Zweckbestimmung erkennen. Noch nicht verifizierbar ist, ob sich die gewünschte bzw. erforderliche Anonymisierung bzw. Pseudonymisierung – auch hier gehen die Meinungen noch auseinander - tatsächlich mit einem ID-Kennzeichen verwirklichen lässt.

Die senatorische Behörde hat mitgeteilt, sie habe meine Bedenken und meine Vorschläge in die Beratungen der KMK eingebracht. Die KMK beabsichtigt mit den Datenschutzbeauftragten der Länder eine einvernehmliche Lösung zu entwickeln. In diesem Sinne ist die Problematik auch auf der Sitzung der Bildungsdeputation im Dezember 2006, auf der ich zu dem Thema vorgetragen habe, erörtert worden.

Das Thema ist auch bundesweit diskutiert worden und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Ende Oktober 2006 hierzu die Entschließung „Keine Schülerstatistik ohne Datenschutz“ (vgl. Ziff. 19.7 dieses Berichts) gefasst. Mit dem Thema befasst sich zudem im ersten Quartal 2007 ein bundesweiter Workshop der KMK unter Beteiligung von Bildungswissenschaftlern, Datenschützern, Statistikern und Journalisten, in dem Argumente für denkbare Modelle erörtert und aus unterschiedlicher Perspektive beleuchtet werden sollen. Auf der Basis der Empfehlungen aus dem Workshop soll über das weitere Vorgehen beraten werden.

13.3 Forschungsvorhaben im Bildungsbereich

Nach § 13 Abs. 6 Bremisches Schuldatenschutzgesetz (BremSchulDSG) bin ich vor der Durchführung von Erhebungen und Untersuchungen zu unterrichten. Innerhalb des Berichtszeitraums habe ich neben den beiden sehr umfangreichen und komplexen Studien „PISA 2006“ (Naturwissenschaften, Leseverständnis und Mathematik) und „IGLU 2006“ (Internationale Grundschul-Lese-Untersuchung) zu weiteren 36 Forschungsvorhaben gegenüber dem Senator für Bildung und Wissenschaft Stellung genommen. Nur im Schulbereich gibt es eine solche Rechtsvorschrift, aufgrund der ich bei Forschungsvorhaben zu beteiligen bin. Darüber hinaus ist vorgesehen, dass Schulen im Rahmen ihres Auftrags zur schulischen Evaluation Untersuchungen zur Überprüfung und des Erfolges ihrer pädagogischen Arbeit vornehmen können, so dass eine weitere Vielzahl von Untersuchungen zu erwarten ist.

Seit 2003 hat jede Dienststelle – auch die Schulverwaltung und die Schulen – einen behördlichen Datenschutzbeauftragten zu bestellen. Aus diesen Gründen habe ich anlässlich der Beratungen zur Novellierung des BremSchulDSG vorgeschlagen, zukünftig den behördlichen Datenschutzbeauftragten der Stelle zu beteiligen, die die Untersuchungen veranlasst bzw. durchführt. Mein Vorschlag wurde aufgegriffen.

Das Spektrum der im Berichtszeitraum durchgeführten Untersuchungen kann der nachfolgenden Aufstellung entnommen werden:

— Umfrage zum Thema Geschlechtskrankheiten und deren Folgen am Lloyd-Gymnasium Bremerhaven,

— Befragung im Rahmen des BLK-Modellversuchs FÖRMIG – Sprachstandsförderung von Kindern und Jugendlichen mit Migrationshintergrund; Teilprojekt SuS (Förderung von Sprachkompetenz und Selbstwirksamkeit),

— Befragung zum Thema „Europäische Union in Bremer Gymnasien“,

— Befragung im Rahmen des Modellversuchs „Demokratie lernen und leben“,

— Datenerhebung in berufsbildenden Schulen zum Thema „Umweltbildung in Berufsschule und Betrieb am Beispiel der Ausbildung von Industriekaufleuten“,

— Genehmigung einer Befragung zum Thema „Lebenswünsche und Lebensziele“,

— Befragung von Schulabgängern über den weiteren beruflichen Werdegang,

— Untersuchung über den weiteren beruflichen Werdegang von Schulabgängern,

— Durchführung einer Lehrerbefragung,

— Genehmigung einer Befragung unter Bremer Chemielehrerinnen und -lehrern,

— Befragung der Schulleitungen zum Thema „Gesundheitsförderung in Schulen“,

— Befragung zum Thema „Verhaltenstraining für Schulanfänger“,

— Antrag auf Genehmigung der Durchführung von Schülerinterviews,

— Studie zu Bullying und Viktimisierung unter Kindern,

— Antrag auf Genehmigung einer Schulleiterbefragung zum Thema „Rauchfreie Schule in Bremen“,

— LBS-Kinderbarometer in Bremen,

— Antrag auf Genehmigung standardisierter Interviews mit Lehrerinnen und Lehrern im Land Bremen zum Thema „Die Rolle der Lehrer/-innen bei der Implementierung und Durchführung von Bildungsreformen“,

— Antrag zur Durchführung einer Umfrage an Berufsschulen,

— Antrag auf Bewilligung einer Erhebung an Bremer Schulen,

— Grundschulstudie TIMSS 2007 („Trends in International Mathematics and Science Study“),

— Datenschutz im Projekt „Projektmanagement im FOS Unterricht“,

— Befragung zum Thema „Wie rechtfertigen Schülerinnen und Schüler Mobbing in der Schule?“,

— Befragung zum Thema „Spielfilmwissen von Schülerinnen und Schülern an deutschen Schulen im Abiturjahrgang“,

— Videostudie zum Lehrerhandeln im Fremdsprachenunterricht,

— Schulbegleitforschung im Rahmen einer integrierten Fördermaßnahme für Schülerinnen und Schüler,

— Befragung zum Thema „Erwachsen werden“,

— Lehrer- und Schülerbefragung zur Nutzung digitaler Medien in Schulen,

— Studie zur Kompetenzentwicklung bei Auszubildenden – Antrag auf Bewilligung des Schulzugangs in Bremen,

— Befragung zum Thema „Probleme sind verkleidete Möglichkeiten – Persönlichkeitsförderung hörgeschädigter Schüler durch Erlebnispädagogik im Unterricht“,

— Antrag auf Genehmigung einer Testdurchführung – Erprobung eines Testinventars im Themenbereich Energie,

— Abschlusserhebung zum BLK-Programm „Demokratie lernen und leben“,

— Befragung von Schülerinnen und Schülern in der Humboldtschule zur Nutzung des Computers und des Internets,

— Befragung zum Thema „Schule im Betrieb (SchuB)“,

— Studie „Wahrnehmung und Beurteilung von Englischlehrwerken aus Schüler- und Lehrerperspektive“,

— Befragung „Formen und Ursachen von Schülergewalt und Maßnahmen der Prävention und Bewältigung“,

— Beantragung einer Studie zum Thema „Motivation und Selbstregulation bei Schülern im Bereich Diagnostik und Interventionsmöglichkeiten“.

13.4 Eingaben aus dem Schulbereich

Datenweitergabe an eine andere Schule durch eine Lehrerin: Eine Lehrerin am Gymnasium Vegesack hatte die Beurteilung eines Schülers ohne elterliche Erlaubnis an eine den Schüleraustausch betreibende Organisation zur Weitergabe an die weiterführende Schule in den USA übermittelt. Auf meine Nachfrage und

den Hinweis auf die Anforderungen des § 3 Abs. 3 Bremisches Datenschutzgesetz (BremDSG) an eine wirksame Einwilligung hat die Schule erklärt, diese Vorgaben zukünftig zu beachten.

Weitergabe einer Bescheinigung über die Kosten einer Klassenfahrt: Die Gaußschule II in Bremerhaven hatte die Bescheinigung über die Kosten einer Klassenfahrt direkt an das Jobcenter Bremerhaven weitergegeben. Auf meine Anfrage hin hat das Schulamt Bremerhaven erklärt, alle Schulen würden nunmehr durch ein Informationsblatt über Schulfahrten und Exkursionen darüber informiert, dass aus Datenschutzgründen alle Schüler ein Exemplar des Vordruckes zur Beantragung von Zuschüssen erhalten sollen. Die betreffende Schule sei noch einmal darauf hingewiesen worden, allen Schülern diesen Vordruck auszuhändigen.

Datenübermittlung von einer Berufschule an einen Arbeitgeber: Der Leiter einer Berufsschule hatte bei einem Auszubildenden ein halbes Gramm Haschisch gefunden und darüber den Ausbildungsbetrieb unterrichtet. Daraufhin wurde das Ausbildungsverhältnis aufgelöst. Das Arbeitszeugnis enthielt den Hinweis, man wünsche ihm für seine berufliche „und private“ Zukunft alles Gute.

Unabhängig davon, ob durch diese Angabe im Arbeitszeugnis die erneute Suche nach einem Ausbildungsplatz mehrfach erfolglos war, habe ich beim Senator für Bildung und Wissenschaft nach der Rechtsgrundlage und Erforderlichkeit dieser Datenübermittlung gefragt. Dieser hat erklärt, es sei unzulässig, derartige Daten an Ausbildungsbetriebe zu übermitteln, und er werde diesen Fall zum Anlass nehmen, auf der Schulleiterbesprechung eindringlich an die Einhaltung der Rechtsvorschriften zu appellieren.

13.5 Dokumentenmanagement-System für Schulen

Das Dokumentenmanagement-System (DMS) ist ein Schulportal des Landesinstituts für Schule (Medien/Landesbildstelle). Lehrkräfte können diese Plattform benutzen, um auf von ihnen selbst eingestellte Dokumente zugreifen zu können. Darüber hinaus können Dateien auch für andere Lehrkräfte und Schülerinnen und Schüler zum Abruf bereitgestellt werden. Hierbei war u. a. beabsichtigt, in einer Logdatei die Zugriffe der registrierten Nutzer (Lehrer, Schüler) zu protokollieren.

Aufgrund meiner Bedenken gegen diese beabsichtigte umfassende Zugriffsprotokollierung wurde auf meinen Vorschlag in den Nutzungsbedingungen festgelegt, unter welchen Voraussetzungen der Provider befugt ist, dort definierte missbräuchliche Nutzungen (z. B. Einstellung jugendgefährdender und rechtwidriger Inhalte und Bilder) zu separieren und innerhalb einer 30-Tage-Frist nur für festgelegte Zwecke an die aufsichtsführenden Stellen für die Lehrkräfte und Schüler zu übermitteln, damit von dort ggf. entsprechende arbeits- bzw. dienstrechtliche oder pädagogische Maßnahmen getroffen werden können. Zugriffe auf die Seiten des Schulportals sollen im Übrigen nur noch zur Bereitstellung des DMS verarbeitet werden.

Ebenso soll auf meine Anregung eine Einverständnis- und Verpflichtungserklärung für die Nutzung des DMS erstellt und von den Nutzern vor der Vergabe einer Zugangsberechtigung unterzeichnet werden, so dass sie die Nutzungsbedingungen anerkennen und über die Protokollierung sowie Regularien bei Verstößen unterrichtet sind.

Des Weiteren sollen auf meine Anregung Bestands- bzw. Zugangsdaten der Nutzer (Name, E-Mail-Adresse, Zugangscode etc.) nur so lange gespeichert werden, bis die Betroffenen das DMS nicht mehr in Anspruch nehmen (Kündigung der Mitgliedschaft etc.). Spätestens 30 Tage danach sind sie zu löschen.

13.6 Bremisches Hochschulreformgesetz

Der Senator für Bildung und Wissenschaft legte im Berichtsjahr den Entwurf des Bremischen Hochschulreformgesetzes (BremHG) vor. Mit dem Gesetz sollen notwendige Rahmenbedingungen geschaffen werden, um den bremischen Hochschulen eine bessere Wahrnehmung ihrer Aufgaben zu ermöglichen. In erheblichem Umfang neu gestaltet wurden dabei auch Regelungen zur Verarbeitung personenbezogener Daten in § 11 BremHG. Sowohl der Kreis der Personen, von denen Daten verarbeitet werden dürfen, als auch die Verarbeitungszwecke wurden erweitert. Der neu gefasste § 11 BremHG soll u. a. auch Regelungen enthalten, die für die Hochschulzulassung, die Berechnung von Lehrverpflichtungen und Leistungsbezügen, die Aufgabenerfüllung des Studentenwerks und die Durchführung des Bre-

mischen Studienkontingentgesetzes erforderlich sind. Innerhalb des durch § 11 BremHG gesetzten Rahmens sollen die Hochschulen die Einzelheiten der Datenverarbeitung selbst festlegen können, ohne dass es noch einer Rechtsverordnung des Senators für Bildung und Wissenschaft hierzu bedarf. Diese Rechtsentwicklung habe ich beratend verfolgt. Ich empfahl dabei u. a., den vorgesehenen Gesetzestext um Verarbeitungszwecke, für die eine personenbezogene Datenverarbeitung erforderlich ist, zu ergänzen und Formulierungen, die den Rahmen hinsichtlich der Betroffenen und der Zwecke zu weit zogen, enger zu fassen. Der Senator für Bildung und Wissenschaft kam meinen Empfehlungen nach. Dabei wurde auf meine Anregung hin in das Bremische Hochschulgesetz auch eine Regelung zur Nutzung der von den Hochschulen bei den Studierenden und Nutzern von Hochschuleinrichtungen erhobenen Daten für die Ausgabe von maschinenlesbaren Hochschulausweisen aufgenommen.

14. Bau, Umwelt und Verkehr

14.1 Dienstanweisung „Korruption“ beim Senator für Bau, Umwelt und Verkehr

Die senatorische Dienststelle hat mir den Entwurf der vorgenannten Dienstanweisung zur Stellungnahme vorgelegt, zu der ich folgende Präzisierungen vorgeschlagen habe:

– Der Kreis der durch mögliche Anzeigen betroffenen Personen darf sich nur auf die Beschäftigten erstrecken, deren Arbeitsplätze als korruptionsanfällig bezeichnet werden.

– Anonyme Anzeigen sollten nur in Ausnahmefällen akzeptiert werden.

– Spätestens nach einem Jahr sollten personenbezogene Daten gelöscht bzw. Untersuchungsergebnisse vernichtet werden, wenn eine Verdachtsvermutung widerlegt werden konnte.

Außerdem wird in der Dienstanweisung die Vertraulichkeit von Hinweisen von Beschäftigten oder Dritten über korruptionsverdächtige Beschäftigte des Ressorts an den Antikorruptionsbeauftragten zugesagt. Hierzu sind meine Vorschläge übernommen worden, wonach der Angezeigte über die Anzeige informiert wird, sobald kein Risiko besteht, dass Beweise vernichtet werden. Der Name des Anzeigenden soll im Regelfall an den Angezeigten nur dann herausgegeben werden, wenn die Anzeige vorsätzlich falsch war.

Diese Regelung ist das Ergebnis einer angemessenen Abwägung zwischen den schutzwürdigen Interessen des Hinweisgebers (Arbeitskollege bzw. Mitarbeiter) vor evtl. Benachteiligungen, z. B. durch seinen Vorgesetzten, und dem berechtigten Interesse des Angezeigten zu erfahren, wer über Hinweise zu seiner Person informiert hat. Zu berücksichtigen ist hierbei auch, dass anonyme Anzeigen bzw. Hinweise nur in Ausnahmefällen akzeptiert werden. Unberührt bleibt jedoch der Auskunftsanspruch nach § 21 Bremisches Datenschutzgesetz (BremDSG), wobei dann im Einzelfall zu klären wäre, ob wegen berechtigter Interessen des Dritten (hier: Hinweisgeber) dessen Name tatsächlich geheimzuhalten ist oder nicht doch der Auskunftsanspruch des Angezeigten überwiegt.

Diese Abwägung entspricht auch der Empfehlung der Arbeitsgruppe „Beschäftigtendatenschutz“ der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich (vgl. Ziff. 18.11 dieses Berichts).

14.2 Prüfung der Verkehrsmanagementzentrale

Im Berichtsjahr habe ich die Videoüberwachung des Straßenverkehrs durch die Verkehrsmanagementzentrale (VMZ) einer Prüfung unterzogen. Der Verkehrsfluss wird über das gesamte Stadtgebiet mit Sensoren oder in die Fahrbahn eingelassenen Messschleifen und an etwa 13 Punkten mit Überwachungskameras beobachtet. Da die Sensoren keinerlei Fahrzeugdaten erfassen, war Gegenstand der Prüfung die Videoüberwachung des fließenden Verkehrs. Den Maßstab gab § 20 b Bremisches Datenschutzgesetz (BremDSG) vor. Die durch die VMZ durchgeführte Videoüberwachung dient der Vervollständigung des aktuellen Verkehrlagebildes an Standorten mit potenziell kritischen Verkehrsverhältnissen.

Die Kameras sind an verschiedenen verkehrsneuralgischen Punkten innerhalb der Stadt installiert. Von der VMZ aus können die einzelnen Kameras in der Regel fern-

gesteuert werden. Die Fernsteuerung umfasst dabei sowohl das Schwenken als auch das Zoomen der Kameras. In der VMZ wird lediglich das aktuelle Bild, das die Kameras liefern, angezeigt. Eine Aufzeichnung der Videosequenzen erfolgt nicht.

Während der Prüfung konnte ich feststellen, dass bei einer Kamera das Zoomen soweit möglich war, dass an einer Ampelkreuzung wartende Personen zu erkennen und Nummernschilder von Fahrzeugen lesbar waren. Bei einer anderen Kamera war das Schwenken soweit möglich, dass auch das Filmen in anliegende Wohnungen bzw. Büroräume möglich wäre. Im Gespräch stellte sich heraus, dass beide Einstellungen für die Aufgabenerfüllung der VMZ nicht benötigt wurden. Dies abzustellen, wurde mir zugesagt.

15. Finanzen

15.1 Gründung der bremischen Niederlassung von Dataport

Im vergangenen Jahr hatte ich über den Beitritt der Freien Hansestadt Bremen zur Anstalt öffentlichen Rechts Dataport berichtet (vgl. 28. JB, Ziff. 15.2). Im Jahr 2006 standen zwei Folgeprojekte an. Zum einen die Weiterentwicklung des IT-Bereichs der bremischen Verwaltung, zum anderen damit verbunden die Gründung einer bremischen Niederlassung des IT-Dienstleisters Dataport in Bremen.

Im ersten Halbjahr ist der bremische IT-Bereich in einer ressortübergreifenden Arbeitsgruppe, an der ich beratend teilgenommen habe, intensiv untersucht worden. Als Ergebnis wurde u. a. festgehalten, bestimmte bisher eher dezentral wahrgenommene IT-Querschnittsaufgaben und die IT-Dienste-Architektur zu bündeln. Die Weiterentwicklung der verwaltungsnahen IT-Dienstleister sollte durch eine neue Ausrichtung der ID Bremen GmbH und der Ausgliederung des Eigenbetriebs Fidatas Bremen als bremische Niederlassung von Dataport erfolgen.

Im zweiten Halbjahr wurden dann die rechtlichen Grundlagen für die vollständige Übertragung des Eigenbetriebs Fidatas Bremen auf Dataport zum 1. Januar 2007 geschaffen. Am 19. Dezember 2006 hat der Senat das von der Bremischen Bürgerschaft beschlossene Gesetz über die Überleitung des Eigenbetriebs Fidatas Bremen auf die Anstalt des öffentlichen Rechts Dataport verkündet (Brem.GBl. 2006, S. 544).

Ich habe den gesamten Prozess begleitet, weil damit natürlich eminent gravierende Veränderungen für die personenbezogene Datenverarbeitung des Landes wie für meine Datenschutzkontrollen verbunden sind.

Zum 1. Dezember 2006 sind die meisten Mitarbeiter der Freien Hansestadt Bremen, die bei der ID Bremen GmbH beschäftigt waren, zur Fidatas Bremen gewechselt und sind somit zu Dataport übergegangen. Dies geht einher mit der Verlagerung der IT-Dienstleistungen auf Dataport, die die ID Bremen GmbH bislang für die Freie Hansestadt Bremen erbracht hat. Nach Abschluss der geplanten Migration der Verfahren bis zum Herbst 2007 wird Dataport damit zum neuen zentralen IT-Dienstleister für die Freie Hansestadt Bremen.

Dieser Prozess, den ich auch während der Migration der Verfahren, die zusätzlich mit einem Umzug in neue Räumlichkeiten verbunden ist, unterstützend begleiten muss, zieht erheblichen Beratungs- und Prüfaufwand, insbesondere aus datenschutztechnischer Sicht nach sich. Denn bei einer Vielzahl auch größerer automatisierter Verfahren, mit denen zum Teil hochsensible personenbezogene Daten verarbeitet werden, kommt es zu einem Wechsel des Auftragnehmers, der durch technische und organisatorische Maßnahmen ein angemessenes Datenschutzniveau zu gewährleisten hat, und zwar auch bei einer Portierung der Verfahren und aller damit verbundenen personenbezogenen Daten. Da die Anstalt öffentlichen Rechts Dataport ein Zusammenschluss von vier Bundesländern ist, ändert sich für mich zudem die Vorgehensweise bei Prüfungen. Insbesondere bei übergreifenden rechtlichen und technischen Fragen im Zusammenhang mit Dataport entsteht die Notwendigkeit, sich mit den anderen Landesbeauftragten für den Datenschutz der beteiligten Bundesländer abzustimmen. Ich habe daher Ende August 2006 mit den Landesbeauftragten für den Datenschutz der Länder Hamburg, Mecklenburg-Vorpommern und Schleswig-Holstein eine Vereinbarung getroffen, in der abgestimmte Verfahrensweisen unter strikter Wahrung der Unabhängigkeit der Landesdatenschutzbeauftragten abgesprochen sind, um gegenüber Dataport eine effektive Datenschutzkontrolle sicherzustellen.

Bereits vor dem Beitritt zu Dataport hatte die Freie Hansestadt Bremen Dataport den Auftrag zur Unterstützung der IT-Steuerverwaltung im Rahmen eines so genannten Data Center Steuern erteilt. Parallel zu den Arbeiten an der Gründung einer bremischen Niederlassung von Dataport wurde im Jahr 2006 das Data Center Steuern errichtet und hat zum 1. Januar 2007 den Betrieb aufgenommen. Die Landesdatenschutzbeauftragten der an Dataport beteiligten Länder haben sich über den Aufbau im Mai 2006 vor Ort bei Dataport informiert und im Anschluss verschiedene datenschutzrechtliche Anforderungen formuliert und diese Dataport mitgeteilt. Es ist notwendig, die Entwicklung weiter zu begleiten.

15.2 Änderung der Steuerdaten-Übermittlungsverordnung

Bis zum 31. Dezember 2005 eröffnete die Steuerdaten-Übermittlungsverordnung übergangsweise die Möglichkeit, eine so genannte qualifizierte elektronische Signatur mit Einschränkungen einzusetzen. Hiergegen hatte sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits im Jahr 2003 wegen der fehlenden umfassenden Sicherheit und der mangelnden Transparenz für die Anwender in einer Entschließung gewandt.

Nach Ablauf der Übergangsvorschrift wurden im Jahr 2006 § 87 a Abs. 6 der Abgabenordnung und die Steuerdaten-Übermittlungsverordnung mit dem Ziel geändert (BR-Drs. 834/06), nunmehr auf Dauer neben der gesetzlich vorgesehenen qualifizierten elektronischen Signatur andere sichere Authentifizierungsverfahren zuzulassen.

Dem ist die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit Entschließung vom 11. Oktober 2006 (vgl. Ziff. 19.5 dieses Berichts) mit Nachdruck entgegengetreten, weil die avisierten Verfahren, etwa aufgrund einer Funktionsvermischung von Signatur- und Authentisierungsfunktion, grundsätzlich ungeeignet oder weniger sicher waren.

Ihre Kritik haben die Datenschutzbeauftragten des Bundes und der Länder auch im Vorfeld dem Bundesministerium der Finanzen und den Landesfinanzministerien mitgeteilt, jedoch im Kern keine Änderungen erreicht. Zuletzt haben sich die Datenschutzbeauftragten vergeblich bemüht zu verhindern, dass für die Bestimmung der Anforderungen bei „anderen sicheren Verfahren“ keine Zustimmung des Bundesamtes für Sicherheit mehr vorliegen muss.

15.3 LUNA – Länderumfassende Namensabfrage zur Betrugsbekämpfung

Zur effektiven Bekämpfung des Umsatzsteuerbetrugs haben die Finanzbehörden des Bundes und der Länder das Verfahren „Länderumfassende Namensabfrage“ (LUNA) entwickelt, das seit dem 1. Januar 2005 bundesweit zur Verfügung steht. Im Jahr 2006 wurde die Version LUNA 2.0 realisiert, bei der die für den Abruf zur Verfügung stehende Datenbasis erweitert und die Zugriffsrechte auf nicht umsatzsteuerspezifische Bereiche ausgedehnt wurde. Zudem machte eine Änderung der Steuerdatenabrufverordnung eine Überarbeitung des Nutzungskonzepts erforderlich.

Im Juli 2006 habe ich gegenüber der bremischen Landesfinanzverwaltung zur Vorbereitung der Bundesarbeitsgruppe Datenschutz der Finanzverwaltungen des Bundes und der Länder zum Nutzungskonzept (Stand: März 2006) Stellung genommen und insbesondere die Begründung der Abfragen und die Protokollierung thematisiert. Nach der Überarbeitung des Nutzungskonzepts habe ich auch zu der neuen Fassung (Stand: September 2006), diesmal für eine koordinierte Stellungnahme gegenüber dem Hessischen Finanzministerium Stellung genommen, und auf verschiedene datenschutzrechtliche Verschlechterungen hingewiesen. Insbesondere war der Umfang der Zugriffsberechtigungen über pauschale Aufgabenzuweisungen (z. B. „Zeitnahe Aufdeckung von Betrugsfällen“, „Bekämpfung der illegalen Beschäftigung“) in einer Weise erweitert worden, die eine differenzierte Vergabe von Zugriffsberechtigungen ausschloss. Der Grund für eine Abfrage sollte zudem bei „Folge- und Detailabfragen“ automatisch übernommen werden, so dass der Zweck des Datenfeldes, die Selbstvergewisserung über den Abfragegrund und die Erforderlichkeit des Abrufs, entfallen würde. Schließlich war die Höchstspeicherdauer von zehn Jahren ohne Grund entfallen.

Der Hessische Datenschutzbeauftragte hat die koordinierte Stellungnahme der Landesbeauftragten für den Datenschutz zur Erstellung eines datenschutzkonformen Nutzungskonzepts dem Hessischen Finanzministerium übermittelt und wird vor Ort die in der Stellungnahme angesprochenen Probleme in einem Gespräch klären.

16. Wirtschaft und Häfen

16.1 Aufzeichnung des Telefonverkehrs durch das HBH

Ende Juli 2006 wandte sich der behördliche Datenschutzbeauftragte vom Hansestadt Bremischen Hafenamt (HBH) an mich und teilte mit, dass beim HBH geplant sei, sämtliche Telefongespräche für spätere Sachverhaltsaufklärungen (Unzulänglichkeiten und evt. Rechtsstreitigkeiten) sowie Fallanalysen aufzuzeichnen.

Ich wies auf das Fernmeldegeheimnis hin, zweifelte die Erforderlichkeit der Aufzeichnung zur rechtmäßigen Erfüllung der Aufgaben des HBH an und wies auf weitere datenschutzrechtliche Anforderungen, u. a. der offenen Erhebung sowie der Unterrichtung der Betroffenen hin. Auch Anrufer oder Angerufene außerhalb des HBH wären von der Gesprächsaufzeichnung betroffen. Ich äußerte erhebliche datenschutzrechtliche Bedenken gegen die Aufzeichnung des Telefonverkehrs und wies darauf hin, dass eine Einwilligung der betroffenen Anrufer und Mitarbeiter fehle und auch eine spezialgesetzliche Rechtsgrundlage, anders als bei Notrufnummern der Polizei und Feuerwehr, nicht bestehe.

Da das HBH an dem Ziel der Aufzeichnung der Telefongespräche festhielt, ging ich in einem weiteren Schreiben näher auf die Anforderungen des Personaldatenschutzes ein, u. a. die Notwendigkeit einer freiwilligen und informierten Einwilligung der Betroffenen. Zugleich wies ich im Fall einer unzulässigen Aufzeichnung von Telefongesprächen auf die Strafbarkeit nach § 201 Abs. 1 Nr. 1 StGB hin.

In einem Gespräch mit dem behördlichen Datenschutzbeauftragten wurde ferner die Notwendigkeit einer Aufzeichnung im Einzelnen erörtert. Ich habe dabei erneut darauf hingewiesen, dass Zwecke der Qualitätssicherung keine lückenlose Aufzeichnung des Telefonverkehrs der Mitarbeiter rechtfertigen, da hierfür in der Einarbeitungsphase ein zeitlich begrenztes und stichprobenartiges Mithören bei Einwilligung der Gesprächsteilnehmer genügt. Ob das Hansestadt Bremische Hafenamt dennoch weiter an der geplanten Aufzeichnung festhält, bleibt abzuwarten.

16.2 Zuverlässigkeitsüberprüfungen nach dem Luftsicherheitsgesetz

Im Laufe des Jahres 2006 wandten sich mehrere Privatpiloten mit verschiedenen Fragen an mich und beklagten die durch § 7 Luftsicherheitsgesetz eingeführte Überprüfung ihrer Zuverlässigkeit. Neben grundsätzlichen Fragen zur Zulässigkeit der Überprüfung und dem rechtlichen Charakter einer Einwilligungserklärung wurde auch bemängelt, dass die Anschreiben mit der Aufforderung, einen Antrag auf Zuverlässigkeitsüberprüfung zu stellen, von der hierfür zuständigen Luftsicherheitsbehörde beim Senator für Wirtschaft und Häfen stammten, die jedoch, anders als die Landesluftfahrtbehörde Bremens, keine Kenntnis vom Innehaben der Fluglizenz haben dürfte.

Nach Gesprächen und Schriftverkehr teilte mir der Senator für Wirtschaft und Häfen schließlich mit, künftig in Gestalt der Landesluftfahrtbehörde die Privatpiloten auf die Rechtsfolgen einer fehlenden Zuverlässigkeitsüberprüfung hinzuweisen und gleichzeitig über die Möglichkeit der Antragstellung bei der Luftsicherheitsbehörde zu informieren.

16.3 Unzulässige Erhebung von Daten zur Anerkennung eines Meisterbriefs

Ein Bürger mit polnischer Staatsangehörigkeit beklagte sich bei mir über die von ihm von der Handwerkskammer Bremen verlangte Bekanntgabe seines Lebenslaufs. Um auch in Deutschland als selbstständiger Handwerksmeister tätig werden zu können, hatte der Petent bei der Handwerkskammer die Anerkennung seines in Polen erworbenen Meisterbriefs beantragt.

Der selbstständige Betrieb eines zulassungspflichtigen Handwerks als stehendes Gewerbe ist nach § 1 Abs. 1 Handwerksordnung (HandwO) nur den in der Handwerksrolle eingetragenen Personen und Personengesellschaften gestattet. Nach § 7 Abs. 1 a HandwO wird in die Handwerksrolle eingetragen, wer in dem von ihm zu betreibenden oder mit diesem verwandten zulassungspflichtigen Handwerk die Meisterprüfung bestanden hat. Im Hinblick auf die Anerkennung im Ausland bestandener Meisterprüfungen gelten darüber hinaus weitere spezielle Vorschriften, nach denen von Antragstellern verschiedene Angaben und Nachweise verlangt werden können. Die Bekanntgabe des Lebenslaufs sehen diese Vorschriften aber nicht vor.

Auf meine Anfrage, weshalb von dem Petenten die Bekanntgabe des Lebenslaufs verlangt werde, erklärte mir dann auch die Handwerkskammer, dass die vorgesehene Erhebung für die Anerkennung des Meisterbriefs nicht erforderlich sei. Benötigt werde in diesem Punkt lediglich eine Aufstellung der beruflich relevanten Tätigkeiten. Hierauf konnte sich der Petent bei seinem Antrag dann auch beschränken. Gleichzeitig wurde das von der Handwerkskammer für die Durchführung derartiger Anerkennungsverfahren entwickelte Merkblatt geändert: Die Forderung „Lebenslauf" wurde durch die Formulierung „Aufstellung der für die Anerkennung/Bewertung relevanten beruflichen Tätigkeiten" ersetzt.

17. Bremerhaven

17.1 Behördenunterlagen mit Schmähungen

Ein Bürger beklagte sich bei mir im Berichtsjahr, er habe in dem Briefkasten seines Hauses Kopien zweier Schreiben gefunden, die er im Hinblick auf eine Abrissverfügung an das Bauordnungsamt Bremerhaven übersandt hatte. Die beiden Schreiben hatte er nicht von der Bauverwaltung zurückerhalten, sondern sie mussten ihm von einem Dritten, vermutlich aus der eigenen Nachbarschaft, in den Briefkasten geworfen worden sein. Sie trugen Eingangsstempel des Bauordnungsamtes und enthielten an einigen Stellen händisch eingefügte Hervorhebungen und handschriftliche abfällige Bemerkungen.

Es konnte nicht geklärt werden, ob die Verwaltung in die Bauakte Dritten (zulässigerweise) Einsicht gewährt hatte. Das Bauordnungsamt darf den an einem Verfahren Beteiligten nach § 29 Abs. 1 i. V. m. § 13 Abs. 1 Bremisches Verwaltungsverfahrensgesetz (BremVwVfG) Akteneinsicht insoweit gewähren, soweit dies zur Geltendmachung oder Verteidigung rechtlicher Interessen erforderlich ist. Die Gewährung der Akteneinsicht nach dem BremVwVfG kann auch die Anfertigung von Kopien aus der Akte umfassen. Das Bauordnungsamt konnte mir aber keine konkrete Auskunft geben, wem und ggf. auf welche Weise im vorliegenden Fall Akteneinsicht gewährt worden war. Es blieb bei der vagen Vermutung, dass die Kopien für einen Berechtigten gefertigt wurden.

Die Entscheidung, ob und inwieweit dem Einsicht Begehrenden von der zuständigen Behörde Akteneinsicht gewährt wird, ist ein Verwaltungsakt und dementsprechend amtlich zu dokumentieren. Das festgestellte Defizit habe ich gegenüber dem Bauordnungsamt gerügt. Meiner Aufforderung einer Dokumentation von Einsichtnahmen durch Dritte will das Amt nachkommen. Es wurden für die Gewährung der Akteneinsicht Merkblätter und Anträge entwickelt, die der Einhaltung der rechtlichen Vorgaben dienen. Auch andere aufgrund dieses Falls in der Zwischenzeit getroffene datenschützende Regelungen sollen eingehalten werden.

17.2 Andere Themen aus Bremerhaven

Da es sich anbietet, viele Themen in einem Sachzusammenhang darzustellen, soll an dieser Stelle die Auffindbarkeit von Beiträgen erleichtert werden, die Themen aus Bremerhaven betreffen. Sie finden sich unter Ziff. 1.1 (Die obersten Datenschutzaufsichtsbehörden kommen in Bremen zusammen), Ziff. 1.6 (Zur Situation der Dienststelle), Ziff. 1.7 (Vorträge, Fortbildungsangebot und Kooperationen), Ziff. 9.2 (Konsequenzen aus dem Urteil zur Rasterfahndung), Ziff. 12.3 (Prüfung der Datenverarbeitung im Dienstleistungszentrum Grünhöfe), Ziff. 13.3 (Forschungsvorhaben im Bildungsbereich), Ziff. 13.4 (Eingaben aus dem Schulbereich), Ziff. 18.3 (Kreditwirtschaft, insbesondere SWIFT), Ziff. 18.10 (Prüfung der Datenverarbeitung in Sanitätshäusern), Ziff. 18.15 (Prüfung der Datenverarbeitung in Fahrschulen), Ziff. 18.18 (Einsatz von Videoüberwachung und Webcams).

18. Datenschutz in der Privatwirtschaft

18.1 Zu den Sitzungen der obersten Datenschutzaufsichtsbehörden

Die Sitzungen des so genannten Düsseldorfer Kreises, dem Zusammenschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich, fanden in diesem Jahr turnusgemäß in Bremen statt. Die dringend einer Verständigung bedürftigen Themen nehmen weiter zu, weil auch in der Privatwirtschaft immer wei-

tere Bereiche mit Informationstechniken automatisiert werden und dabei in zunehmendem Maße personenbezogene Daten, sei es der Beschäftigten, sei es der Kunden, in vielfältiger Weise mit einbezogen werden. Hinzu treten ein ansteigender Vertrieb von Waren, Dienstleistungen und Informationen über das Internet, die zunehmende Internationalisierung der Datenverarbeitung oder die technische Entwicklung neuer IT-Produkte, aber auch eine fortschreitende Vernetzung in der Wirtschaft und die Entstehung neuer Datenverbünde.

So waren denn die jeweils über 40 Punkte enthaltenden Tagesordnungen der Sitzungen des Düsseldorfer Kreises trotz straffer Führung nicht abzuarbeiten. Eine Darstellung würde den Bericht sprengen, auch wenn ich mich nur auf eine kurze Beschreibung beschränken würde. Allein das 60-seitige Protokoll der Frühjahrssitzung spricht Bände. Ich will an dieser Stelle daher exemplarisch nur einige Themenschwerpunkte des Düsseldorfer Kreises nennen:

Fragen des internationalen Datenverkehrs, wie Übermittlung sensitiver Daten an Auftragnehmer in Drittstaaten, exterritoriale Anwendbarkeit des Bundesdatenschutzgesetzes (BDSG), Unternehmensregelungen zum Datenschutz, Standardvertragsklauseln, das Vertragsverletzungsverfahren der EU-Kommission gegen die Bundesrepublik Deutschland wegen Verstoßes gegen die EG-Datenschutzrichtlinie;

verschiedene Themen betreffend die Auskunfteien, hier z. B. Online-Auskunft über „MeineSCHUFA.de“, Nutzung von Daten aus dem Inkasso-Bereich für die Auskunftserteilung oder erweitertes Online-Auskunftsverfahren bei Online-Krediten;

die Kreditwirtschaft, hier z. B. Bonitätsanfragen durch Kreditinstitute ohne Einwilligung des Betroffenen, Datenübermittlung der SWIFT-Zentrale in Belgien an die USA, Weiterleitung von Bankverbindungsdaten des Überweisenden an den Begünstigten wie auch Fragen zum Scoring;

die Versicherungswirtschaft, hier u. a. Datenaustausch zwischen Versicherungen und Außendienstmitarbeitern, Gespräche beim Bundesverband Verbraucher-Zentrale e. V. über eine Einwilligungserklärung in der Versicherungswirtschaft oder Fragen der Benachrichtigung Dritter bei der Einmeldung in ein zentrales Warnsystem der Versicherungswirtschaft;

Fragen des Arbeitnehmerdatenschutzes, hier insbesondere Fragen von so genannten Whistleblowing-Hotlines und die Initiative zur Aufnahme von Vorschriften zum Arbeitnehmerdatenschutz in ein Arbeitsgesetzbuch;

verschiedene Fragen im Zusammenhang mit der Datenverarbeitung bei der Personenüberprüfung und dem Ticketing bei der Fußballweltmeisterschaft 2006;

verschiedene Fragen betreffend die Rechtsstellung und Aufgaben von betrieblichen Datenschutzbeauftragten, hier insbesondere Auslegung der neuen Regelungen im Mittelstandsentlastungsgesetz;

den Bereich Verkehr, hier Fehler- und Unfalldatenspeicher in Kraftfahrzeugen, Aufzeichnung telefonischer Taxibestellungen oder Datenschutz im öffentlichen Personennahverkehr;

Fragen der Datenschutzaufsicht bei Rechtsanwälten und Datenschutz bei Detekteien, Speicherfristen aufgrund des Allgemeinen Gleichbehandlungsgesetzes (AGG) sowie Fragen der Datenverarbeitung bei Markt- und Meinungsforschung.

Hervorheben möchte ich, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), der mittlerweile in einer ganzen Reihe von Feldern eigene Zuständigkeiten gegenüber Unternehmen der Privatwirtschaft hat, in 2006 volles Mitglied des Düsseldorfer Kreises geworden ist. Ein Durchbruch gelang auch bei der Informationspolitik des Düsseldorfer Kreises. War es bisher so, dass die Entscheidungen lediglich den Parteien in der Wirtschaft mitgeteilt wurden, die es anging, in der Regel also Wirtschaftsverbände und Dachorganisationen, hat sich der Düsseldorfer Kreis jetzt auf Regularien verständigt, um Beschlüsse auch der Öffentlichkeit zugänglich zu machen. Sie werden unter www.bfdi.bund.de für jedermann im Internet abrufbar zur Verfügung gestellt.

18.2 Voraussetzungen für den Einsatz von RFID-Chips

RFID-Systeme bestehen aus einem mobilen Datenspeicher (Transponder) und einem Lese- und/oder Schreibsystem. Sie dienen dazu, Gegenstände zu kennzeichnen. Die Technik ermöglicht die eindeutige Identifizierung eines Gegenstands. Auf

dem Chip können je nach Leistungsfähigkeit verschiedene Informationen gespeichert und ggf. auch verändert werden. Die Bauformen der Bestandteile eines RFID-Systems können sehr unterschiedlich sein, in der Regel sind sie aber sehr klein. Für die Übermittlung der Daten über Funkwellen stehen verschiedene Frequenzbereiche zur Verfügung. Einfache Anwendungen befinden sich z. B. in Zugangssystemen wie den Fußballtickets zur WM 2006, in Skipässen oder Autoschlüsseln. Ein erheblich größeres Potenzial steckt jedoch im Einsatz der Technik bei der Kennzeichnung von Bauteilen und Einzelprodukten, weshalb RFID besonders für Produktion, Logistik und Handel von Interesse ist. Die RFID-Technologie wird den Barcode ersetzen, aber auch Anwendungen im medizinischen Bereich oder auch Autonummernschilder sind schon im Einsatz.

Die RFID-Technologie steht erst am Anfang ihrer Entwicklung. Dabei geht man davon aus, dass in einer parallelen Welt der Dinge diese untereinander kommunizieren und sich selbstständig organisieren (z. B. der Kühlschrank bestellt den fehlenden Aufschnitt). Schon jetzt spricht man von einem Internet der Dinge, auch dem Web 2. Die mit der Technologie verbundenen neuen Möglichkeiten und Veränderungen, insbesondere aber die möglichen Arbeitserleichterungen und Kosteneinsparpotenziale werden dafür sorgen, dass diese Mikrochips in fast allen Bereichen zum Einsatz kommen werden. Ich erwarte eine rasche Verbreitung binnen kürzester Zeit. RFID wird alle Lebensbereiche durchdringen. Deshalb ist es wichtig, in der jetzigen Entwicklungsphase, in der noch gestaltend eingegriffen werden kann, die technischen Vorkehrungen zu implementieren, die das informationelle Selbstbestimmungsrecht der von dieser Technologie betroffenen Besitzer stärken. Darüber hinaus bleibt abzuwarten, ob die derzeitigen rechtlichen Regelungen ausreichen, um den Datenschutz auch beim Einsatz dieser Technologie zu garantieren. Gegebenenfalls muss der Gesetzgeber durch ergänzende rechtliche Regelungen die Hersteller und die Wirtschaft, die sich für den Einsatz dieser Technologie entscheidet, verpflichten, dass diese ausreichende Potenziale zur Sicherung des Datenschutzes zur Verfügung stellen. Es geht dabei nicht um die Verhinderung dieser Technologie, sondern um ihre Gestaltung. Die Datenschutzaufsichtsbehörden haben hierzu in Bremen einen Beschluss gefasst, in dem sie die notwendigen Parameter für die Entwicklung und den Einsatz der Technologie festlegen (vgl. Ziff. 20.2 dieses Berichts). Dieser Beschluss ist den einschlägigen Organisationen und Verbänden der Wirtschaft übermittelt worden und ich hoffe, dass er genügend Anreiz für weitere Diskussionen gibt.

18.3 Kreditwirtschaft, insbesondere SWIFT

Im Bereich der Kreditwirtschaft hat es verschiedene Aktivitäten auf Bundesebene gegeben. Unter anderem war auch eine Bürgereingabe aus Bremerhaven Auslöser für die Überprüfung der Praxis des Umfangs der Datenübermittlung an den Empfänger bei Überweisungen. Nach von mir geführten Verhandlungen mit dem führenden norddeutschen Rechenzentrum der Kreditwirtschaft wird die Frage nun mit dem Zentralen Kreditausschuss der Deutschen Kreditwirtschaft (ZKA) weiterverhandelt. Der Vorgang ist noch nicht abgeschlossen.

Hohe Wellen schlug die Mitteilung, dass die in Belgien ansässige SWIFT (Society for Worldwide Interbank Financial Telecommunication), über die weltweit der gesamte internationale Zahlungsverkehr der Banken abgewickelt wird, die dabei anfallenden Daten im SWIFT-Rechenzentrum in den USA spiegelt und dort den US-amerikanischen Behörden und dem Geheimdienst in vollem Umfang Daten zugänglich macht. Diese Praxis ist sowohl nach deutschem als auch nach EU-Datenschutzrecht unzulässig. Rechtlich verantwortlich sind dabei neben der SWIFT-Zentrale auch die deutschen Banken. Diese bündeln ihre Interessenvertretung im ZKA. Die Datenschutzaufsichtsbehörden haben in einem gemeinsamen Beschluss (vgl. Ziff. 20.1 dieses Berichts) die Praxis für rechtlich unzulässig erklärt und die Banken aufgefordert, unverzüglich Maßnahmen zu ergreifen. Der ZKA wurde von mir über diesen Beschluss unterrichtet. Wenig später hat auch die Artikel-29-Datenschutzgruppe der EU mit ähnlichem Inhalt dazu einstimmig die Stellungnahme WP128 verabschiedet.

18.4 Eingaben gegen die Handels- und Wirtschaftsauskunfteien

Erneut erhielt ich eine Vielzahl von Eingaben, die sich gegen die Speicherung und Datenweitergabe von Auskunfteien richteten. Soweit ich nicht unmittelbar helfen konnte, z. B. weil anderenorts Feststellungen gemacht werden mussten, gab ich die

Eingaben an die Datenschutzaufsichtsbehörden ab, in deren Zuständigkeitsbereich die Auskunfteien ihren Sitz haben. Mehrere Eingaben, die die Verarbeitung personenbezogener Daten durch in Bremen ansässige Wirtschaftsauskunfteien betrafen, verfolgte ich selbst. Die Bürger beklagten sich dabei u. a., dass über sie unrichtige Daten hinsichtlich ihrer wirtschaftlichen Betätigung gespeichert, ihnen zustehende Betroffenenauskünfte nicht oder nicht rechtzeitig erteilt oder aber zu beachtende Löschfristen nicht eingehalten würden. Nach den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) dürfen über den Betroffenen nur richtige Daten gespeichert werden. Außerdem hat der Betroffene einen umfassenden Auskunftsanspruch, dem auch die Auskunfteien gerecht werden müssen.

Zu diesen Eingaben führte ich Prüfungen bei den betreffenden Auskunfteien durch. Soweit sich hierbei die von den Petenten geschilderten Mängel bestätigten, gelang es, dass die Auskunfteien die von ihnen gespeicherten Daten berichtigten bzw. löschten oder aber die erbetenen Auskünfte erteilten.

18.5 Bericht zur Arbeitsgruppe Versicherungswirtschaft

Die Mitglieder der AG Versicherungswirtschaft haben sich im Berichtsjahr zu drei Sitzungen getroffen. Beraten wurden u. a. strittige Punkte mit der Versicherungswirtschaft, die die Verhandlungen ins Stocken gebracht hatten. Dies waren u. a. die aufgrund von Rechtsprechung notwendig gewordenen Änderungen der Einwilligungsklausel nach dem Bundesdatenschutzgesetz, die Frage der Benachrichtigung Dritter bei der Einmeldung in das Versicherungsinformationssystem Uniwagnis, die Zulässigkeit von Bonitätsauskünften an Versicherungen und Fragen des Scoring in der Versicherungswirtschaft.

Außerdem wurden folgende Themen beraten: die Übernahme von Geschäftstätigkeiten innerhalb einer Versicherungsgruppe, die Frage des Umfangs zulässiger Datenübermittlungen zwischen Versicherungswirtschaft und Auskunfteien sowie die Frage der Übermittlung von Arztberichten an Krankenversicherungsunternehmen.

Viele der Themen waren auch Gegenstand der Behandlungen in den Sitzungen der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich (Düsseldorfer Kreis) in Bremerhaven und Bremen. Schließlich soll nicht unerwähnt bleiben, dass Mitte des Jahres der Vorsitz in der AG Versicherungswirtschaft von Hamburg auf das Unabhängige Landeszentrum für Datenschutz (ULD) in Schleswig-Holstein übergegangen ist.

18.6 Telefongesprächsaufzeichnung bei Schadensmeldung in der Versicherungswirtschaft

Ein Rechtsanwalt wies mich auf folgende Praxis hin: Sein Mandant habe seine Versicherung über einen Zentralruf über einen Rechtsschutzfall telefonisch informiert. Zunächst sei ihm von dort eine Deckungszusage gemacht worden. Wenige Tage später habe ihn sein örtlich zuständiger Versicherungsvertreter angerufen und ihm erklärt, er habe in dem fraglichen Fall keinen Anspruch auf Versicherungsschutz. In dem Telefonat mit dem Versicherungsvertreter seien die Worte hin und her gegangen, schließlich habe der Vertreter ihm gegenüber erklärt, er, der Versicherungsunternehmer, habe „das und das“ gesagt, er habe noch einmal in sein Gespräch mit dem Versicherungsunternehmen hineingehört.

Der Versicherungsnehmer war erstaunt, dass sein Telefongespräch ohne sein Wissen aufgezeichnet worden war. Auf Rat des Rechtsanwalts wies er seinen Versicherungsagenten darauf hin, dass die Praxis der Gesprächsaufzeichnung nicht zulässig sei. Ihm wurde daraufhin in dem fraglichen Fall eine Deckungszusage erteilt mit der Maßgabe, den Fall nicht „an die große Glocke zu hängen“. Bei diesem Gespräch sei ihm deutlich gemacht worden, dass es wohl in der gesamten Versicherungsbranche gängige Praxis sei, telefonische Schadensmeldungen aufzuzeichnen. Wegen der Besonderheit des Falles bat der Rechtsanwalt, das fragliche Versicherungsunternehmen noch nicht bekannt zu geben, um Schaden von seinem Mandanten abzuwenden.

Wegen der behaupteten generellen Praxis in der Versicherungswirtschaft habe ich angeregt, die Frage mit dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) zu erörtern. Aus meiner Sicht sollte dabei überlegt werden, wie dem Interesse der Versicherungswirtschaft einerseits und der Unterrichtung und Transparenz für den Betroffenen vor einer möglichen Aufzeichnung andererseits Rech-

nung getragen werden kann. So könnte ein dem Gespräch vorgeschalteter Sprachcomputer eingesetzt werden, mit dem die Versicherungswirtschaft ermittelt, ob der Betroffene mit einer Aufzeichnung des Gesprächs einverstanden ist oder nicht. Alternativ könnte auch eine bloße Ansage vorgeschaltet werden, die darauf hinweist, dass das Gespräch aufgezeichnet werden soll und er seine Entscheidung dem Sachbearbeiter mitteilen soll. Der Sachbearbeiter könnte dann bei Zustimmung die Aufzeichnung manuell starten.

Weiter habe ich, um einen Ausgleich zu erreichen, angeregt, durch Verfahrensregelungen zu ermöglichen, solche Aufzeichnungen auf Wunsch auch den jeweiligen Versicherten zugänglich zu machen. In jedem Fall muss festgelegt sein, wer zu welchen Zwecken solche Gesprächsaufzeichnungen im Unternehmen nutzen darf. Voraussetzung hierfür wäre eine revisionssichere Speicherung der Aufzeichnung. Innerhalb des Versicherungsunternehmens müssen die aufgezeichneten Gespräche einem Zugriffsschutz unterliegen, um die Gefahr des Missbrauchs zu minimieren. Weiterhin wären Löschfristen für die Gesprächsmitschnitte und die zugehörigen Protokolldaten zu definieren und umzusetzen.

18.7 Mittelstandsentlastungsgesetz

Ende August 2006 trat das Erste Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft (BGBl. I S. 1970) in Kraft. Durch das Artikelgesetz wurden auch verschiedene Regelungen des Bundesdatenschutzgesetzes (BDSG) geändert.

Im Wesentlichen geht es um die Erhöhung des Schwellenwertes für die Ausnahme von der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten von derzeit vier auf nunmehr neun Mitarbeiter, die mit der Verarbeitung personenbezogener Daten beschäftigt sind. Entsprechend trifft auch die Meldepflicht für automatisierte Verfahren nur noch Unternehmen, die mehr als neun Mitarbeiter besitzen, die mit der Verarbeitung personenbezogener Daten beschäftigt sind. Ferner können externe Datenschutzbeauftragte, die bei Berufsgeheimnisträgern eingesetzt sind, sich auf ein abgeleitetes Zeugnisverweigerungsrecht berufen. Andererseits unterliegen sie nun auch der Strafandrohung bei Verletzung von Amts- und Berufsgeheimnissen (§ 203 Abs. 1 StGB). Klargestellt wird, dass die erforderliche Fachkunde des betrieblichen Datenschutzbeauftragten abhängig vom Umfang der Datenverarbeitung und dem Schutzbedarf der personenbezogenen Daten ist. Für die Datenschutzaufsichtsbehörden wird neben der Kontrollfunktion explizit neu eine Beratungsfunktion für betriebliche Datenschutzbeauftragte festgelegt. Aus Sicht der Datenschutzaufsichtsbehörden stellt sich das Gesetz als Abbau von Schutzvorschriften dar, ohne dass der angestrebte Entlastungseffekt für die mittelständische Wirtschaft erkennbar ist. So befreit die Lockerung von der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten die nicht öffentliche Stelle nicht von den inhaltlichen Anforderungen an den Datenschutz. Diese gelten unverändert und in vollem Umfang und sind durch den Leiter der Stelle in anderer Weise sicherzustellen. Daher wird es absehbar für die Aufsichtsbehörden zu mehr Beratungsaufwand kommen. Zwar enthält das Gesetz einige Klarstellungen, jedoch auch verschiedene neu zu bestimmende Rechtsbegriffe, die neuen Klärungsbedarf aufwerfen.

18.8 Weitergabe von Patientendaten durch den Insolvenzverwalter einer Pflegeeinrichtung

Mit einer Eingabe wurde mir zur Kenntnis gebracht, dass der Insolvenzverwalter einer ambulanten Pflegeeinrichtung, ein Rechtsanwalt aus Bremen, eine Liste mit den Daten aller von der insolventen Pflegeeinrichtung betreuten Patienten an die Arbeitsgemeinschaft der Krankenkassenverbände in Bremen und an eine Krankenkasse geschickt hatte, um für den Fall, dass ein Versicherungsverhältnis besteht, die Begleichung etwaiger offener Rechnungsbeträge zu erreichen. Tatsächlich bestand jedoch nur ein Versicherungsverhältnis mit einer einzigen Patientin.

Unter Hinweis darauf, dass es sich bei der Offenlegung der Eigenschaft der Pflegebedürftigkeit einer Vielzahl von Patienten um ein unbefugtes Offenbaren von Gesundheitsdaten handelt, forderte ich ihn zur Stellungnahme auf. Er trug vor, aufgrund fehlenden Personals keine Möglichkeit gehabt zu haben festzustellen, bei welcher Krankenkasse die Patienten jeweils versichert sind. Vor dem Hintergrund, dass durch einfache Einsicht in die Unterlagen bzw. Kontaktaufnahme mit den Pa-

tienten die Frage nach deren Krankenversichertenverhältnissen hätte geklärt werden können, leitete ich ein Ordnungswidrigkeitsverfahren gegen den Insolvenzverwalter ein.

18.9 Personenverwechslung bei der Ausstellung eines Rezepts

Im Rahmen meiner Bürgersprechstunde wandte sich eine Frau an mich, der von einem Versicherungsunternehmen eine für sie ausgestellte ärztliche Verordnung zugeschickt worden war. Das Versicherungsunternehmen, das im Übrigen keine Krankenversicherungssparte hat, teilte ihr mit, dass das Rezept zu dem Versicherungsunternehmen fehlgeleitet worden sei. Die ärztliche Verordnung war mit einem Apothekenstempel versehen, was die Aushändigung des Medikaments nahelegt. Es handelte sich dabei um ein Medikament gegen Wechseljahrebeschwerden, das sich die Frau jedoch nie hat verschreiben lassen, zumal sie es in ihrem Alter gar nicht benötigt. Bei dem ausstellenden Arzt war sie ebenfalls nicht gewesen. Auch die naheliegende Vermutung, ihre Versichertenkarte sei in fremde Hände gelangt, konnte sie ausschließen. Ich rief den Arzt an, in dessen Praxis das Rezept ausgestellt worden war, berichtete ihm den Sachverhalt und bat ihn um Aufklärung. Er bestätigte mir, das Rezept für die Frau ausgestellt zu haben und vermutete zunächst, dass diese in Vertretung für eine von ihm genannte Gynäkologin in seiner Praxis gewesen sei und er ihr ohne Untersuchung das Rezept ausgestellt habe. Eine Rücksprache bei der Petentin ergab zwar, dass sie bei der vom ausstellenden Arzt genannten Gynäkologin in Behandlung sei, die Praxis des Arztes jedoch hatte sie niemals betreten. Ich rief daher die Gynäkologin an, die sich sehr verwundert zeigte, da der Arzt für sie keine Vertretung durchführe. Stattdessen führe er für sie Zelluntersuchungen durch, wie auch im Fall der genannten Patientin. Zu diesem Zweck habe sie dem Arzt die Daten der Beschwerdeführerin übermittelt. Sie bestätigte auch, dass ihre Patientin das verschriebene Medikament nicht benötige. Kurz darauf meldete sich der Arzt, der zwischenzeitlich mit der Gynäkologin gesprochen hatte, erneut und konnte die Angelegenheit endlich aufklären: Es hatte in seiner Praxis eine Verwechslung mit einer anderen Patientin mit gleichem Nachnamen gegeben. Diese sei bei ihm Privatpatientin und habe das verschriebene Medikament auch bekommen.

18.10 Prüfung der Datenverarbeitung in Sanitätshäusern

Im Berichtsjahr habe ich die Datenverarbeitung in Sanitätshäusern in Bremerhaven und Bremen geprüft. Bei der Bestellung und dem Verkauf von Sanitätsartikeln werden Daten über den Gesundheitszustand der Kunden verarbeitet. Es handelt sich hierbei im Wesentlichen um Daten, die sich auf den Rezepten befinden. Diese sind im Einzelnen: Name der Krankenkasse, Name, Adresse und Geburtsdatum der Kunden, Kassen-Nummer, Versichertennummer, Versichertenstatus, Vertragsarztnummer, Gültigkeitsdatum der Versichertenkarte, Ausstellungsdatum, verordnetes Hilfsmittel und Diagnose.

Diese Daten werden elektronisch und in Papierform gespeichert. Die Speicherung dient der Erstellung der Kostenvoranschläge für die Krankenkassen und der Abrechnung. Die elektronisch erstellten Abrechnungen enthalten nur für die Abrechnung relevante Daten, die Diagnose wird darin z. B. nicht mehr genannt. Sowohl die Aufbewahrung und Versendung der Rezepte mit der Bezeichnung der verordneten Hilfsmittel und den Diagnosen als auch die Speicherung der ausgelieferten Hilfsmittel im System stellen eine Verarbeitung von Gesundheitsdaten dar, die nach § 3 Abs. 9 Bundesdatenschutzgesetz (BDSG) zu den besonderen Arten von Daten zählen und deshalb einer besonderen Schutzbedürftigkeit unterliegen.

Ich konnte feststellen, dass die durch die Sanitätshäuser erhobenen Daten für die Versorgung mit Hilfsmitteln erforderlich waren. Die Papierunterlagen wurden für den erforderlichen Zeitraum sicher aufbewahrt und nach der Auslieferung der Hilfsmittel datenschutzgerecht vernichtet. Auch elektronisch wurden nur die für die Erfüllung des Vertragsverhältnisses erforderlichen Daten verarbeitet. Hier habe ich auf der Ebene der technischen Datenschutzmaßnahmen die Absicherung des EDV-Netzes gegenüber unbefugten Zugriffen und die Möglichkeiten der für die Sanitätshäuser speziell entwickelten Fachanwendungen geprüft. Hierzu gehörte die Zugangskontrolle (Anlage § 9 BDSG) zum System, die über angemessene Authentisierungsmechanismen (Benutzername, sicheres Passwort) gewährleistet werden muss. Ebenso geprüft wurden die Verfügbarkeitskontrolle, d. h., der Schutz von Kunden-

daten gegen zufällige Zerstörung oder Verlust, die Zugriffskontrolle (wer von den Mitarbeitern darf mit welchen Funktionen auf die Kundendaten zugreifen) und insgesamt die Absicherung gegenüber dem Internet.

Ich konnte eine Reihe von wirkungsvollen technischen Schutzmaßnahmen feststellen. Dazu gehörten u. a. Maßnahmen zur physikalischen, unwiderruflichen Löschung der Daten auf den Festplatten, Maßnahmen zum Schutz des In-House-Netzes gegenüber externen Anschlüssen durch die Bildung eines Grenznetzes, Einsatz von Schutzsoftware zur Erkennung von Viren, Spyware und Trojanern, Firewallfunktionen sowie verschlüsselte Datenspeicherung.

Mängel konnte ich bei organisatorischen Maßnahmen erkennen, wie etwa die vorgeschriebene Dokumentation der technischen und organisatorischen Maßnahmen im Rahmen einer Verfahrensbeschreibung (§ 4 e Abs. 1 BDSG). Auch gab es im Fall eines an das Internet angeschlossenen Stand-alone-Rechners keine eindeutig sichere Trennung von im Rahmen eines Terminkalenders eingetragenen Kundendaten. Allerdings waren hier keine Diagnosen gespeichert. Es bestand aber die Möglichkeit, über dort eingetragene Tätigkeiten mit vorhandenem Zusatzwissen auf die Art der gesundheitlichen Störung zu schließen. In einem anderen Fall wurden für den Betrieb der Fachanwendung noch DOS-PC verwendet, die über deutlich weniger Sicherheitsmaßnahmen verfügen als Windows-Systeme. Beispielsweise kann jede Person, die Zugang zu diesem Rechner hat, diesen auch administrieren, also z. B. Einstellungen ändern und Software einspielen. Auch Auftragsverhältnisse zu Supportfirmen mussten hinsichtlich der Handhabung personenbezogener Daten präzisiert werden.

Insgesamt wurde bis auf die oben genannten Mängel ein angemessenes, z. T. hohes Datenschutzniveau vorgefunden. Die Sanitätshäuser wurden im Rahmen der von mir zugestellten Prüfberichte aufgefordert, die festgestellten Mängel zu beseitigen.

18.11 Konzeption eines Arbeitsgesetzbuches und Arbeitnehmerdatenschutz

Im August 2006 hat das Forschungsinstitut für Deutsches und Europäisches Sozialrecht an der Universität Köln im Auftrag der Bertelsmann Stiftung den Diskussionsentwurf eines Arbeitsvertragsgesetzes (ArbVG) vorgelegt. Im Vorfeld dazu hatten mehrere Aufsichtsbehörden für den Datenschutz – auch die in Bremen – unter Federführung der Aufsichtsbehörde Nordrhein-Westfalen dem Institut Vorschläge zur Aufnahme von Regelungen zum Arbeitnehmerdatenschutz unterbreitet. Grundlage waren die Beschlüsse der Konferenz der Datenschutzbeauftragten „zum Datenschutz im Recht des öffentlichen Dienstes“ und „zum Arbeitnehmerdatenschutz“ aus den Jahren 1991 und 1992 sowie das Datenschutzniveau des Bundesdatenschutzgesetzes, der Landesdatenschutzgesetze sowie der Beamtengesetze des Bundes und der Länder.

Leider enthält der Diskussionsentwurf nur einzelne Datenschutzregelungen, z. B. zur Datenerhebung im Bewerbungsverfahren und eine allgemeine Regelung zur Einsicht in Personalakten. Erhebliche Bedenken bestehen gegen eine Schlussvorschrift, wonach erlaubt werden soll, dass zu Ungunsten des Arbeitnehmers per Tarifvertrag, Betriebsvereinbarung oder Arbeitsvertrag von Bestimmungen des Gesetzes abgewichen werden kann. Es ist im Datenschutzrecht unumstritten, dass derartige Regelungen das gesetzliche Datenschutzniveau nicht unterschreiten dürfen.

Die Projektverantwortlichen des Instituts rechnen mit einer weiterhin regen Beteiligung von Interessengruppen (Verbände, Gewerkschaften, Berufsvereinigungen etc.) und haben dargelegt, es sei hilfreich, wenn die Aufsichtsbehörden für den Datenschutz ihre Vorstellungen zum Arbeitnehmerdatenschutz mitteilen könnten und um ergänzende Vorschläge gebeten. Das wird zu prüfen sein. Das Institut hat unter der Homepage www.arbvg.de ein Portal eingerichtet, in dem sich interessierte gesellschaftliche Gruppen und Personen zu dem Entwurf äußern können.

18.12 Meldung unzulässiger Verhaltensweisen im Betrieb durch Beschäftigte (Whistleblowing)

In zunehmendem Maße setzen international tätige Unternehmen Whistleblowing Hotlines ein, die auch für die jeweiligen Niederlassungen in Deutschland – also auch im Land Bremen – gelten sollen. Zwecke dieser Hotlines sind u. a., Unregelmäßigkeiten im Finanzsektor oder Korruptionsfälle aufzudecken. Wegen der Unsicherhei-

ten über die Zulässigkeit dieser Hotlines und zur Wahrung der schutzwürdigen Interessen Betroffener vor unzulässiger Denunziation etc. hat die Arbeitsgruppe „Beschäftigtendatenschutz“ der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich ein Papier erarbeitet, das für Unternehmen, Personalvertretungen und Betroffene eine Orientierungshilfe darstellen soll. Es berücksichtigt die Stellungnahme 1/2006 bzw. WP117 der Artikel-29-Datenschutzgruppe (Datenschutzbeauftragte der Mitgliedstaaten der EU), abrufbar unter www.europa.eu.int/comm/justice-home/fsj/privacy/docs/wpdocs/2006/wp117-de.pdf. Das nationale Arbeitspapier wird zurzeit noch im Kreise der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich abgestimmt.

Rechtsgrundlage für derartige Hotlines ist § 28 Abs. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG), wonach derartige Hotlines zulässig sind zur Wahrung der berechtigten Interessen der Unternehmen, Regelverstöße aufzudecken oder zu vermeiden. Hierbei dürfen jedoch die schutzwürdigen Interessen der Beschäftigten, über die von anderen Kollegen Meldungen erfolgen, nicht überwiegen.

Als zulässige Zwecke kommen Verhaltensweisen in Betracht, die einen sich gegen das Unternehmensinteresse richtenden Straftatbestand erfüllen (z. B. Korruption und Unterschlagung) oder Verhaltensweisen, die gegen die Menschenrechte verstoßen (z. B. Ausnutzung günstiger Produktionsbedingungen im Ausland durch in Kauf genommene Kinderarbeit und Umweltverstöße). Nicht dagegen sind Verhaltensweisen als Regelverstöße zu betrachten, die unternehmensinterne Verhaltensregeln beeinträchtigten, wie z. B. ein unzulässiges Verbot privater Kontakte unter Beschäftigten.

Eine Regelung über derartige Hotlines sollte den angesprochenen Personenkreis und den Zweck der jeweiligen Hotline konkret bestimmen. Außerdem müssen die Beschäftigten über Zweck, Organisation und Nutzungsbedingungen sowie Auskunfts-, Berichtigungs- und Löschungsrechte der Betroffenen unterrichtet werden. Anonyme Anzeigen (auch Hinweise) sollten nur in Ausnahmefällen akzeptiert werden. Anonymität widerspricht dem Transparenzgebot und begünstigt gegenüber der namentlichen Nennung eher Missbrauch und Denunziation. Durch anonyme Hinweise gemeldete Personen können sich gegen eine etwaige Verleumdung in einem rechtsstaatlichen Verfahren nicht wehren. Den Hinweisgebern muss verdeutlicht werden, dass ihre Identität den Personen, die an weiteren Überprüfungen oder ggf. anschließend eingeleiteten Gerichtsverfahren beteiligt sind, enthüllt werden kann. Dies gilt hinsichtlich entsprechender Akteneinsichtsrechte in evtl. Strafverfahren. Eine betroffene Person ist erst dann über Anzeigen zu informieren, wenn kein Risiko besteht, dass Beweise für ein Fehlverhalten vernichtet werden oder ein Missbrauch der Hotline offensichtlich ist. Außerdem sollten die Daten innerhalb von zwei Monaten nach Abschluss der Untersuchung gelöscht werden.

Bedeutsam ist auch, dass vor dem Einsatz eines derartigen automatisierten Verfahrens wegen der besonderen Risiken für die Rechte und Freiheiten der Betroffenen eine Vorabkontrolle durch den Beauftragten für den Datenschutz vorgenommen wird und entsprechende technische und organisatorische Maßnahmen zur Wahrung der Vertraulichkeit (z. B. Einsatz von Verschlüsselungsverfahren) und der Löschungsverpflichtung getroffen werden.

18.13 E-Mail-Weiterleitung nach Ausscheiden aus dem Betrieb

Die Weiterleitung von E-Mails nach Ausscheiden eines Mitarbeiters aus dem Unternehmen ist grundsätzlich zulässig, wenn die E-Mail-Nutzung nur zu betrieblichen Zwecken erlaubt und die Nutzung zu privaten Zwecken ausdrücklich untersagt worden ist. Allerdings ist nicht auszuschließen, dass trotzdem private E-Mails über die personengebundenen E-Mail-Adressen von Mitarbeitern eingehen. Diese unterliegen dem Fernmeldegeheimnis nach § 88 Telekommunikationsgesetz (TKG), wonach dem Arbeitgeber nicht erlaubt ist, Einsicht in private E-Mails zu nehmen.

Hierbei sind die Voraussetzungen des § 28 Abs. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) zu beachten. Zur Wahrung der schutzwürdigen Interessen eines ausscheidenden Mitarbeiters aus dem Unternehmen sollte folgende Vorgehensweise beachtet werden:

Wenn ein Mitarbeiter das Unternehmen verlässt, sollte er vorher die in seinem E-Mail-Fach vorhandenen persönlichen bzw. privaten E-Mails löschen, während die betrieblichen E-Mails entweder an den Vertreter oder Nachfolger weitergeleitet

oder ggf. ebenfalls gelöscht werden, soweit sie für betriebliche Zwecke nicht mehr benötigt werden.

Sollte dies z. B. bei einer fristlosen Kündigung nicht mehr möglich sein, hängt es von den jeweiligen Umständen des Einzelfalls ab, ob eine Einsichtnahme in das E-Mail-Fach erforderlich ist, um betriebliche E-Mails bearbeiten zu können. Hierbei empfiehlt es sich, eine verantwortliche Person zu bestimmen, die zur Wahrung der schutzwürdigen Interessen des ehemaligen Mitarbeiters nur Einsicht in das E-Mail-Fach nimmt, um betriebliche E-Mails auszusortieren und offensichtlich private E-Mails unverzüglich zu löschen.

Nach dem Ausscheiden eines Mitarbeiters aus dem Unternehmen sollte die E-Mail-Adresse unverzüglich gelöscht werden, so dass keine weiteren E-Mails mehr unter dieser Adresse eingehen. Alternativ besteht die Möglichkeit, über den Abwesenheitsassistenten den Hinweis anzubringen, dass unter dieser E-Mail-Adresse keine E-Mails mehr bearbeitet werden und auf eine andere E-Mail-Adresse zu verweisen.

18.14 Weitergabe von Personalakten

Eine Vielzahl von Beschäftigten eines privatrechtlich organisierten Unternehmens hatte moniert, ihre Personalakten seien an eine Dienststelle der bremischen Verwaltung weitergegeben worden, ohne dass sie darüber informiert oder gar ihre Einwilligungen eingeholt worden wäre.

Das Unternehmen hat erklärt, die Weitergabe sei auf Anforderung der Dienststelle zur Rückführung der Beschäftigten in den bremischen Dienst erforderlich gewesen. Die die Personalakten anfordernde Dienststelle hat auf Anfrage erklärt, nur mit Hilfe der Personalakten sei eine qualifikationsorientierte Rückführung und Einweisung der Beschäftigten möglich. Eine Aufstellung erforderlicher Daten sei für diesen Zweck nicht ausreichend gewesen.

Das Unternehmen hat daraufhin auf Anfrage zugesichert, in ähnlich gelagerten Fällen des § 28 Abs. 3 Nr. 1 Bundesdatenschutzgesetz (BDSG) zukünftig die Beschäftigten unmittelbar nach der Weitergabe ihrer Personalakten darüber zu informieren.

18.15 Prüfung der Datenverarbeitung in Fahrschulen

Im Berichtsjahr habe ich die Verarbeitung personenbezogener Daten von Fahrschülern in den Geschäftsräumen von fünf Fahrschulen geprüft. Bei den Prüfungen sind jeweils die Formulare „Ausbildungsvertrag“, „Antrag auf eine Fahrerlaubnis“ und eine „Bewerberliste“ zur Anmeldung von Führerscheinprüfungen an den Technischen Überwachungsverein (TÜV) Nord vorgelegt worden.

Zu den rechtlichen Anforderungen: Rechtsgrundlagen zur Zulässigkeit der Datenverarbeitung sind § 28 Abs. 1 Nr. 1 Bundesdatenschutzgesetz (BDSG) und § 18 Fahrlehrergesetz (FahrlG) i. V. m. § 6 Durchführungsverordnung zum Fahrlehrergesetz (FahrlGDV) einschließlich der Anlagen 3 und 4 (Ausbildungsnachweis und Tagesnachweis für Fahrlehrer). Die Fahrschule schließt mit einer/einem sich meldenden Fahrschülerin/Fahrschüler einen Ausbildungsvertrag ab. Hierzu wird ein Formular verwendet, in das die erforderlichen Daten (Stammdaten und andere) eingetragen werden.

Zweifel an der Zulässigkeit der Datenverarbeitung habe ich hinsichtlich des Datums „Staatsangehörigkeit“ bei einer Fahrschule in Bremerhaven geäußert. Hierzu erklärte der Fahrlehrer, dieses Datum benötige die Fahrerlaubnisbehörde. Diese würde ggf. beim Ausländeramt nachfragen, ob eine befristete oder unbefristete Aufenthaltsgenehmigung vorliege. Auf Anfrage hat die Fahrerlaubnisbehörde mitgeteilt, diese Angabe sei nie von dort verlangt worden. Daraufhin hat der Fahrlehrer erklärt, dieses Datum zukünftig nicht mehr zu erheben.

Bei einer anderen Fahrschule sind in der Datenmaske eines Fahrlehrerprogramms die Felder „Staatsangehörigkeit“ und „Sprache“ aufgeführt. Dort wurde die jeweilige Sprache des Fahrschülers in das Feld „Staatsangehörigkeit“ eingetragen. Die Aufnahme der Sprache ist stets freiwillig und deshalb bedeutsam, weil die Fahrprüfer den Fahrschülern ermöglichen wollen, die schriftliche Prüfung in ihrer Muttersprache abzulegen. Wegen des Grundsatzes der Richtigkeit der Daten habe ich empfohlen, die Sprache in das entsprechende Feld einzutragen und das Feld „Staatsangehörigkeit“ zu löschen. Die Fahrschule hat dies zugesagt.

Die im Ausbildungsvertrag enthaltenen Daten werden bei allen geprüften Fahrschulen elektronisch gespeichert und nach Abschluss der Fahrausbildung bzw. nach Bestehen der Fahrprüfung zehn Jahre lang aufbewahrt. Diese Frist ergibt sich aus § 257 Abs. 4 Handelsgesetzbuch (HGB).

Ich habe Zweifel geäußert, ob auch die elektronisch gespeicherten Daten neben den übrigen Unterlagen in Papierform zehn Jahre lang aufbewahrt werden müssen. Die Fahrschulen haben jeweils zugesagt zu klären, ob die Daten nach zwei bis drei Jahren gelöscht werden können, so dass nur noch die in Papierform zur Steuerprüfung zu verwendenden Daten zehn Jahre lang aufbewahrt werden. Da diese Unterlagen Belege i. S. des § 257 Abs. 1 Nr. 4 HGB sind, werden sie von allen Fahrschulen in Papierform aufbewahrt.

Technische Sicherungsmaßnahmen: Die für die Erfüllung des Ausbildungsvertrages erforderlichen Daten wurden bei allen geprüften Fahrschulen elektronisch auf Stand-alone-Rechnern unter dem Betriebssystem Windows XP oder Rechnern mit Internet-Zugang mit unterschiedlichen Fachanwendungen für Fahrschulen verarbeitet, teilweise mit einer Online-Verbindung zum TÜV Nord zur Terminbestellung. Diese Online-Verbindung war datenschutzgerecht abgesichert.

Bei den Prüfungen wurden von mir außerdem Fragen zur Zugangskontrolle einer angemessenen Authentifizierung und Verfügbarkeitskontrolle, d. h., dem Schutz der Fahrschülerdaten gegen zufällige Zerstörung oder Verlust, geklärt.

Zur Zugangs-, Zugriffs- und Weitergabekontrolle nach Nrn. 2 bis 4 und 7 der Anlage zu § 9 Satz 1 BDSG habe ich bei einer Verbindung der Rechner mit dem Internetanschluss der Fahrschule die Installation einer „Personal Firewall“ empfohlen. Sie ermöglicht u. a., die Zugänge zum Rechner und die auf den Festplatten der Rechner gespeicherten Programme zu schützen. Auch ein Virenschutz zur Prüfung von E-Mail-Attachments ist dort in der Regel integriert. Informationen über entsprechende Produkte finden sich auch im Internet; für grundlegende Informationen über „Personal Firewalls“ habe ich auf meine Homepage www.datenschutz.bremen.de verwiesen.

18.16 Bonitätsprüfung bei der Bezahlung von Parkgebühren per Handy

Durch einen Pressebericht der Bremer Tageszeitungen wurde ich darauf aufmerksam, dass in Bremen die Bezahlung von Parkgebühren per Handy ermöglicht werden soll. Ich nahm daraufhin Kontakt mit der Firma auf, um mich über die geplanten Datenverarbeitungsvorgänge unterrichten zu lassen. Die Firma erklärte mir in diesem Zusammenhang, neben der Übermittlung von personenbezogenen Daten an die beteiligten Banken, Kreditkartenunternehmen und Mobilfunknetzbetreiber des Nutzers sei auch eine Überprüfung der Kreditwürdigkeit bei Auskunfteien vorgesehen. Grundlage für die Bonitätsprüfung seien §§ 28, 29 Bundesdatenschutzgesetz (BDSG). Um die wirtschaftliche Situation eines Unternehmens bei Kleinbetragsgeschäften nicht zu gefährden, müsse eine entsprechende Prüfung des Nutzers auf sein Bezahlverhalten vor Geschäftsabschluss erfolgen. Bei Nichtzahlung mit anschließender Verfolgung (Mahnwesen, Vollstreckung usw.) stehe der Aufwand in keinem wirtschaftlichen Verhältnis zum Ertrag. Keine Verfolgung fordere zum Missbrauch durch den Nutzer auf. Eine Prüfung des Zahlungsverhaltens sei daher immer vor der Gewährung des „Kredites“ zwingend. Außerdem informiere sie den Nutzer darüber, dass im Falle der Nichteinlösung der Lastschrift diese Tatsache in eine Sperrdatei aufgenommen werde, so dass er faktisch bis zur Begleichung der Forderungen von zukünftigen Zahlungen per Handy ausgeschlossen werde. Das Unternehmen berief sich dabei auch auf seine im Internet veröffentlichten Allgemeinen Geschäftsbedingungen (AGB).

Da wohl kein Nutzer, der mit seinem Fahrzeug auf einen Parkplatz fährt, vor der Bezahlung zunächst im Internet nach den AGB der Firma sucht, wäre die Bonitätsprüfung ohne Wissen und Kenntnis hinter dem Rücken der Betroffenen vonstatten gegangen und schon allein aus diesem Grund unzulässig. Weiter ist zu beachten, dass die Datenerhebung bei anderen Personen oder Stellen nur zulässig wäre, wenn sie zur Wahrung des Geschäftszwecks erforderlich wäre und keine Anhaltspunkte dafür bestünden, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt würden (§ 28 Abs. 1 Nr. 2 i. V. m. § 4 Abs. 2 b BDSG). Es ist zumindest strittig, ob Kleinstbeträge zum Anlass einer Bonitätsprüfung dienen dürfen. Im vorliegenden Fall war ohnehin beabsichtigt, säumige Nutzer in eine Sperrdatei aufzunehmen.

Zu einer Klärung dieser Fragen kam es nicht, weil zwischenzeitlich das Unternehmen aus wirtschaftlichen Gründen diesen Dienst einstellen musste, weil dieser von zu wenig Kunden in Anspruch genommen wurde. Die beteiligten Geschäftspartner erklärten dann auch, sie wollten kein Nachfolgeprojekt auflegen.

18.17 Herausgabe von Mitgliederdaten an Vereinsmitglieder und Dritte

Im vergangenen Jahr haben sich verschiedentlich Vereine und Vereinsmitglieder mit datenschutzrechtlichen Fragestellungen an mich gewandt. Dabei ging es z. B. um die datenschutzkonforme Gestaltung der Vereinssatzung und der Einwilligungsklauseln in den Beitrittserklärungen oder um die Rechtmäßigkeit der Übermittlung von Mitgliederdaten an andere Vereine und Verbände.

Ein weiteres Dauerthema ist die Herausgabe von Mitgliederdaten an Vereinsmitglieder zum Zweck der Kontaktaufnahme oder zur Wahrnehmung von satzungsmäßigen Rechten, etwa der Einberufung außerordentlicher Mitgliederversammlungen oder der Ergänzung der Tagesordnung.

So haben sich Mitglieder eines als Verein geführten Kindergartens an mich gewandt und um Mitteilung gebeten, ob ihnen vom Vorstand des Vereins eine Mitgliederliste zur Verfügung zu stellen ist, um die Vereinsmitglieder im Vorfeld einer Mitgliederversammlung über einen Tagesordnungspunkt zu informieren und ggf. einen abweichenden Antrag zu formulieren. Nach Einsicht in die Satzung des Vereins ergab sich, dass Anträge zur Behandlung in der Tagesordnung der Mitgliederversammlung ohne Quorum gestellt werden konnten. Eine Mobilisierung der Mitglieder und Übersendung der Mitgliederdaten war daher nicht erforderlich. Die Bestimmungen der Satzung ließen sich zudem dahin auslegen, dass fristgerecht eingegangene Anträge im Vorfeld der Mitgliederversammlung an alle Mitglieder zu versenden waren. Damit war auch ausgeschlossen, dass eine ad-hoc Behandlung von Gegenanträgen auf der Mitgliederversammlung, zu der mangels näherer Kenntnis unter Umständen nur ein Teil der Mitglieder erscheint, zu verfälschten Ergebnissen führt.

In einem ähnlichen Fall hat das Amtsgericht Bremen mit Urteil vom 28. November 2005 (Az. 1 C 0061/05), bestätigt durch Beschluss des Landgerichts Bremen vom 1. Juni 2006 (Az. 1 S 406/05), die Klage eines Vereinsmitglieds als unbegründet zurückgewiesen, das auf Herausgabe bzw. Bekanntgabe einer Namen und Anschriften enthaltenen Mitgliederliste eines Vereins geklagt hatte, dessen Ziel die Aufklärung zu gesundheitlichen Risiken sowie die Verbesserung der Vorsorge und Unterstützung Betroffener ist. Das Gericht hat anerkannt, dass zur Durchsetzung der Einberufung einer außerordentlichen Mitgliederversammlung eine Kommunikation zwischen den Vereinsmitgliedern zur Mobilisierung von Mitinteressenten nötig ist. Nach Auffassung des Gerichts gewährleistete der Verein diese Kommunikation jedoch durch ein Rundbriefverfahren. Zudem überwog das Datenschutzinteresse der Vereinsmitglieder vorliegend das berechtigte Interesse an der Herausgabe der Mitgliederliste, da aufgrund der Thematik des Vereins davon auszugehen war, dass ein Teil der Mitglieder persönlich betroffen ist und in hohem Maße Anspruch auf sensiblen Umgang mit ihren Daten hatte. Eine Umfrage unter den Mitgliedern hatte ergeben, dass nur ein Bruchteil der Datenweitergabe zustimmte. Die Klägerin selbst gehörte nicht dazu.

Aufgrund des anhaltend hohen Beratungsbedarfs habe ich in Zusammenarbeit mit verschiedenen anderen Landesbeauftragten für den Datenschutz bereits im Jahr 2002 ein Faltblatt „Datenschutz im Verein“ erstellt und im Anschluss daran eine ausführlichere Broschüre „Datenschutz im Verein“, in der sich u. a. auch Beispielsformulierungen für eine Datenschutzregelung in der Satzung und das Muster einer Einwilligungserklärung befinden. Die Broschüre ist auf meiner Webseite www.datenschutz.bremen.de abrufbar.

18.18 Einsatz von Videoüberwachung und Webcams

Im letzten Jahr erreichten mich mehr als 20 Anfragen, die sich gegen die Videoüberwachung von Wohn- und Geschäftsgebäuden wandten. Es wäre zu aufwändig, jeden Fall hier ausführlich darzustellen, so dass ich mich auf einige exemplarische Fälle beschränke.

In Spielhallen: Ein Kunde beschwerte sich z. B. über das Vorhandensein von Kameras in einer Spielhalle, sowohl in den Kabinen als auch am Geldwechselautomat.

Das Unternehmen erklärte, die Videoüberwachung sei vorwiegend zur Abschreckung von Übergriffen oder Manipulationen in den Kabinen und am Geldwechselautomat durch Gäste erforderlich. Darüber hinaus verlangten die Berufsgenossenschaften aufgrund der besonderen Gefahrensituation in Spielstätten die Videoüberwachung. Meine Aufforderung ist umgesetzt worden, an mehreren Stellen entsprechende Hinweise anzubringen.

Eingang und Fahrstuhl eines Wohn- und Geschäftshauses: Eine Einwohnerversammlung einer Großwohnanlage hatte per Mehrheitsbeschluss über den Einsatz der Videoüberwachung entschieden. Daraufhin haben mehrere Eigentümer und Mieter dargelegt, dadurch würden ihre schutzwürdigen Interessen beeinträchtigt; außerdem würden regelmäßig Patienten einer in der Wohnanlage befindlichen Arztpraxis überwacht werden.

Der Beschluss einer Eigentümerversammlung ist keine Befugnis zur Videoüberwachung. Entscheidend ist, ob eine Vorabkontrolle zum Ergebnis hat, dass die materiell- und formalrechtlichen Voraussetzungen des § 6 b Bundesdatenschutzgesetz (BDSG) vorliegen bzw. eingehalten werden. Insbesondere wegen der schutzwürdigen Interessen der die Arztpraxis aufsuchenden Patienten ist, neben den allgemeinen Anforderungen, auf meine Empfehlung hin festgelegt worden, die Videoüberwachung nur außerhalb der Geschäftszeiten dieser Praxis zu aktivieren.

Kamera-Attrappen: Aufgrund der Hinweise von Passanten auf eine an einem Wohngebäude angebrachte auf die öffentliche Straße gerichtete Videokamera hat die Hausverwaltung auf Nachfrage erklärt, es handele sich um eine Attrappe, die den gewünschten Abschreckungseffekt gegen Einbruch und Vandalismus entfalte. Auf meinen Vorschlag hin wurde die Attrappe ausschließlich auf den zum Privatgrundstück gehörenden Eingangsbereich gerichtet und ein Hinweis auf den Umstand der Videoüberwachung angebracht.

Die zumindest analoge Anwendung des § 6 b BDSG ist insbesondere aufgrund des Urteils des Landgerichts Bonn vom 16. November 2006 (Az. 8 S 1389/04) angemessen. Das Gericht kommt zu dem Schluss, die Attrappe einer Kamera erwecke den Eindruck der Überwachung, der den gleichen Überwachungsdruck auslöse wie eine echte Kamera, aber auch die gleiche abschreckende Wirkung habe. Soweit die Attrappe auf den öffentlichen Straßenraum gerichtet sei, beeinträchtige sie das Persönlichkeitsrecht des Betroffenen ebenso wie es echte Kameras täten.

Webcams auf Baustellen: Mehrere Hinweise auf diese Webcams waren verbunden mit der Befürchtung, hier würden die Bauarbeiter einer permanenten Kontrolle durch den Arbeitgeber ausgesetzt sein. Hierzu habe ich die jeweils angegebenen Webcams auf den Homepages angesehen (z. B. Neubau eines Kultur- und Dienstleistungszentrums in der Bremerhavener Innenstadt und der Neubau von Radio Bremen in der Faulenstraße). Zweck dieser Webcams ist, regelmäßig die Öffentlichkeit über den Fortschritt von Neubauten zu informieren.

Es handelte sich in beiden Fällen um feststehende Bilder, die erst nach ca. 15 bis 30 Minuten aktualisiert wurden. Keine Bedenken bestehen, wenn die Personen auf der Baustelle nicht erkennbar sind und nur feststehende Bilder, die in länger andauernden Intervallen aktualisiert werden, veröffentlicht werden. Abgesehen davon kann jeder betroffene Beschäftigte direkt bei den Baufirmen Auskunft nach § 34 Bundesdatenschutzgesetz (BDSG) darüber erhalten, ob und ggf. zu welchen Zwecken die Firmen ihre Bilddaten verarbeiten. Außerdem muss die Baufirma als Arbeitgeberin die auf ihrer Baustelle tätigen Beschäftigten nach § 4 Abs. 3 BDSG über die Zwecke etwaiger Videoaufnahmen unterrichten.

18.19 Ordnungswidrigkeitsverfahren

In zwei Fällen verhängte ich im Berichtsjahr nach § 43 Bundesdatenschutzgesetz (BDSG) Bußgelder wegen begangener Ordnungswidrigkeiten. In einem Fall war das betroffene Unternehmen mehrfach meiner Aufforderung nicht nachgekommen, zu einer Eingabe, die ich zuvor erhalten hatte, Stellung zu nehmen. Die dem Unternehmen übersandten Anschreiben wurden nicht beantwortet, obwohl es gem. § 38 Abs. 3 Satz 1 BDSG hierzu verpflichtet war. Der Bußgeldbescheid ist zwischenzeitlich rechtskräftig geworden. Da das Unternehmen nicht bereit war, in der ihm dafür eingeräumten Frist das verhängte Bußgeld zu entrichten, ist das Mahn- und Beitreibungsverfahren eingeleitet worden.

In dem anderen Fall übermittelte ein Insolvenzverwalter vorsätzlich unzulässigerweise eine Vielzahl von Daten pflegebedürftiger Personen an eine Krankenkasse, was einen Verstoß gegen § 28 Abs. 6 BDSG darstellt (vgl. Ziff. 18.8 dieses Berichts). Gegen den gegen ihn verhängten Bußgeldbescheid hat der Insolvenzverwalter Einspruch eingelegt. Der Bußgeldvorgang ist zur weiteren Bearbeitung an die Staatsanwaltschaft Bremen abgegeben worden.

19. Die Entschließungen der Datenschutzkonferenzen im Jahr 2006

19.1 Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

(Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006)

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

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

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

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

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

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

———

*) KOM (2005) 475 vom 4. Oktober 2005.

19.2 Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht

(Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006)

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

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

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

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

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

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

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

Es wird deshalb gefordert, dass nur die personenbezogenen Daten erhoben werden, die für die Vergabe unbedingt erforderlich sind. Rechtlich problematisch ist insbesondere die vorgesehene Erhebung und Verarbeitung der Pass- bzw. Personalausweisnummer der Karteninteressentinnen und -interessenten. Der Gesetzge-

ber wollte die Gefahr einer Nutzung der Ausweis-Seriennummer als eindeutige Personenkennziffer ausschließen. Die Seriennummer darf damit beim Ticketverkauf nicht als Ordnungsmerkmal gespeichert werden. Zur Legitimation der Ticketinhaberin bzw. -inhabers beim Zutritt zu den Stadien ist sie nicht erforderlich. Das Konzept der Ticket-Vergabe sollte daher überarbeitet werden. Eine solche Vergabepraxis darf nicht zum Vorbild für den Ticketverkauf auf Großveranstaltungen werden. Solche Veranstaltungen müssen grundsätzlich ohne Identifizierungszwang besucht werden können.

19.3 Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige

(Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006)

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

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

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

19.4 Keine datenschutzkontrollfreien Räume bei der Leistung von ALG II

(Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006)

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

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

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

lich. Sie würde den Grundrechtsschutz der betroffenen Bürgerinnen und Bürger empfindlich beeinträchtigen.

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

19.5 Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 im Umlaufverfahren – bei Enthaltung von Schleswig-Holstein)

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

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

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

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

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

Wird ein Authentisierungsschlüssel zum Signieren verwendet,

— kann fälschlicher Weise behauptet werden, dass Nutzende elektronische Dokumente signiert haben; da sie das Gegenteil nicht beweisen können, müssen sie befürchten, die damit verbundenen Rechtsfolgen tragen zu müssen,

— besteht die Möglichkeit, dass Authentisierungsverfahren (Single Sign On, Challenge Response etc.) gezielt missbräuchlich verwendet werden,

— wird den Nutzenden keine „Warnfunktion“ mehr angeboten wie bei der ausschließlichen Verwendung des Signaturschlüssels zum Signieren und

— sind die Verfahren und die daraus resultierenden Konsequenzen für die Nutzenden nicht mehr transparent.

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

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

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

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

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

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

19.6 Verbindliche Regelungen für den Einsatz von RFID-Technologien

(Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006)

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

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

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

Das Bundesverfassungsgericht hat den Gesetzgeber mehrfach darauf hingewiesen, dass wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwicklungen aufmerksam zu beobachten sind und notfalls durch ergänzende Rechtsetzung korrigierend einzugreifen ist. Da-

her sind die besonderen Gegebenheiten, die mit dem Einsatz der RFID-Technologie verbunden sind, vom Gesetzgeber daraufhin zu untersuchen, ob für alle Risiken adäquate und rechtliche Schutzmechanismen vorhanden sind. In den Bereichen, in denen diese fehlen, hat der Gesetzgeber einzugreifen. Dies gilt insbesondere für den Fall, dass die Hersteller und Anwender sich auf eine verbindliche Selbstverpflichtung nicht einlassen.

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

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

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

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

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

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

19.7 Keine Schülerstatistik ohne Datenschutz

(Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006)

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

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

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

Im Übrigen sind folgende verfassungsrechtliche Vorgaben und Grenzen unabdingbar:

— Der Umfang des Erhebungsprogramms ist auf den für die Statistikzwecke dienlichen Umfang zu beschränken.

— Bei allen Festlegungen sind die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit zu beachten.

— Bei der Datenverarbeitung ist das Gebot der personellen, organisatorischen, räumlichen und verfahrensmäßigen Trennung von Verwaltungsvollzug und Statistik einzuhalten und das Statistikgeheimnis zu gewährleisten.

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

19.8 Das Gewicht der Freiheit beim Kampf gegen den Terrorismus

(Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006)

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

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

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

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

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

19.9 Verfassungsrechtliche Grundsätze bei Antiterrordatei-Gesetz beachten

(Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006)

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

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

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

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

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

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

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

Die zugriffsberechtigten Sicherheitsbehörden sind nicht klar genug bezeichnet. Aufgrund der Speicherung auch höchst sensibler personenbezogener Vorfelddaten muss der Gesetzgeber aus rechtsstaatlichen Gründen selbst festlegen, welche Stellen zugriffsberechtigt sein sollen.

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

20. Die Beschlüsse der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich

20.1 SWIFT: Datenübermittlung im SWIFT-Verfahren in die USA

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 8./9. November 2006 in Bremen)

Es wird festgestellt, dass die gegenwärtige Spiegelung von Datensätzen im SWIFT-Rechenzentrum in den USA und die anschließende Herausgabe von dort gespeicherten Daten an US-amerikanische Behörden wegen fehlender Rechtsgrundlage sowohl nach deutschem Recht als auch nach EG-Datenschutzrecht unzulässig ist.

Insbesondere verfügen die USA über kein angemessenes Datenschutzniveau im Sinne des Artikel 25 Abs. 1 und Abs. 2 der EG-Datenschutzrichtlinie. Rechtlich verantwortlich für die Übermittlung der Daten in die USA sind sowohl die in Belgien ansässige SWIFT, als auch die deutschen Banken, die sich trotz des Zugriffs der amerikanischen Behörden auf die bei SWIFT/USA gespeicherten Datensätze auch weiterhin der Dienstleistungen von SWIFT bedienen.

Die Banken werden aufgefordert, unverzüglich Maßnahmen vorzuschlagen, durch die im SWIFT-Verfahren entweder eine Übermittlung von Daten in die USA unterbunden werden kann oder aber zumindest die übermittelten Datensätze hinreichend gesichert werden, damit der bislang mögliche Zugriff der US-amerikanischen Sicherheitsbehörden künftig ausgeschlossen ist. Eine Möglichkeit besteht nach Ansicht der Aufsichtsbehörden in der Verlagerung des zurzeit in den USA gelegenen Servers in einen Staat mit einem angemessenen Datenschutzniveau. Eine weitere Möglichkeit besteht in einer wirksamen Verschlüsselung der in die USA übermittelten Zahlungsverkehrsinformationen. Es muss ausgeschlossen sein, dass die US-amerikanischen Behörden in die Lage versetzt sind, die auf dem dortigen Server gespeicherten Datensätze zu dechiffrieren. Die Aufsichtsbehörden erwarten eine ernsthafte Auseinandersetzung der Banken mit den aufgezeigten Möglichkeiten. Allgemeine Hinweise auf eine faktische oder ökonomische Unmöglichkeit sind nicht akzeptabel. Der Verweis auf einen in der Zukunft liegenden und noch keinesfalls feststehenden Abschluss eines völkerrechtlichen Abkommens zwischen dem EU-Rat und der US-Regierung vermag nicht den gegenwärtigen Handlungsbedarf zu beseitigen.

Unabhängig davon müssen die Banken gemäß § 4 Abs. 3 Bundesdatenschutzgesetz ihre Kundinnen und Kunden darüber informieren, dass im Falle der Weiterleitung von grenzüberschreitenden Zahlungsaufträgen die Datensätze auch an ein in den USA ansässiges SWIFT Operating Center übermittelt werden. Dabei bleibt es den Banken überlassen, ob sie alle Kundinnen und Kunden über die Übermittlung der Datensätze an SWIFT/USA informieren oder nur diejenigen, für die die Dienste von SWIFT genutzt werden. Die Unterrichtung der Kundinnen und Kunden ist eine notwendige, wenn auch nicht hinreichende Mindestvoraussetzung für die Zulässigkeit der Übermittlung der Daten an SWIFT/USA. Sie ist unverzüglich umzusetzen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich nehmen das Anliegen der deutschen Banken zur Kenntnis, aus Gründen des Wettbewerbs eine europaweit einheitliche Lösung zu erreichen. Es soll in Zusammenarbeit mit den übrigen europäischen Datenschutz-Aufsichtsbehörden eine einheitliche Handhabung angestrebt werden.

20.2 Die Entwicklung und Anwendung von RFID-Technologie ist insbesondere im Handel und im Dienstleistungssektor datenschutzkonform zu gestalten!

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 8./9. November 2006 in Bremen)

Die gegenwärtige Entwicklung der RFID-Technologie (Radio Frequency Identification) und ihr Einsatz im Handel und im Dienstleistungssektor kann Kosteneinsparungspotenziale beispielsweise im Rahmen von Logistik- und Produktionsprozessen eröffnen. Sie birgt allerdings auch erhebliche Risiken für das Persönlichkeitsrecht von Verbraucherinnen und Verbrauchern. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich halten es deswegen für erforderlich, dass die RFID-Technologie datenschutzkonform entwickelt und eingesetzt wird. Bereits jetzt sollten Hersteller und Anwender im Handel und im Dienstleistungssektor die Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie nutzen.

RFID ist eine Technik, um Daten mit Hilfe von Funkwellen auf einem Chip berührungslos und ohne Sichtkontakt lesen, speichern und gegebenenfalls verarbeiten zu können. Mit RFID-Chips gekennzeichnete Gegenstände können mit einem Lesegerät abhängig von der Reichweite bzw. Sendestärke identifiziert und lokalisiert werden. Ungeachtet der zahlreichen Vorteile des Einsatzes von RFID-Chips ist zu befürchten, dass zukünftig massenhaft personenbezogene Daten verarbeitet werden, indem nahezu alle Gegenstände des täglichen Lebens (einschließlich Kleidung, Lebensmittel- und andere Verpackungen, Medikamente usw.) über Hintergrundsysteme dauerhaft den Betroffenen zugeordnet werden können. RFID ermöglicht damit technisch die von den Verbraucherinnen und Verbrauchern unbemerkte Ausforschung ihrer Lebensgewohnheiten und ihres Konsumverhaltens etwa zu kommerziellen Zwecken.

Diese technologische Entwicklung stellt den Datenschutz vor neue Herausforderungen. Ob auf RFID-Chips gespeicherte Daten einen Personenbezug aufweisen, wird häufig von den konkreten Umständen des Einzelfalls abhängen. Selbst Informationen, die zunächst keinen Personenbezug haben, weil sie allein ein Produkt kennzeichnen, könnten über die Lebensdauer des Chips gesehen – zum Beispiel mit Hilfe von Hintergrundsystemen – später einer konkreten Person zugeordnet werden. Damit würden rückwirkend alle gespeicherten Daten über einen mit einem RFID-Chip gekennzeichneten Gegenstand zu personenbezogenen Daten. Ein datenschutzkonformer Einsatz der RFID-Technologie wird deshalb immer schwerer kontrollierbar sein. Die Ausübung der verfassungsrechtlich begründeten, datenschutzrechtlich unabdingbaren Rechte der Verbraucherinnen und Verbraucher auf Auskunft sowie auf Löschung und Berichtigung von unrichtigen personenbezogenen Daten wird – insbesondere wegen der geringen Größe der RFID-Chips – künftig erheblich erschwert.

Angesichts dieses Gefährdungspotenzials der RFID-Technologie erscheint es fraglich, ob die bestehenden gesetzlichen Regelungen ausreichen, den wirksamen Schutz der Persönlichkeitsrechte der Betroffenen zu gewährleisten.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich halten es für erforderlich, dass bereits bei der technologischen Ausgestaltung von RFID das Recht auf informationelle Selbstbestimmung der Betroffenen gewahrt wird. Dazu gehört vor allem, dass Verbraucherinnen und Verbrauchern nach dem Kauf von Produkten die RFID-Chips auf einfache Weise unbrauchbar machen können. Daneben sind auch die Datenschutzrechte der betroffenen Arbeitnehmerinnen und Arbeitnehmer im Produktions- und Logistikprozess zu wahren. Zugleich sind unter anderem der Handel und der Dienstleistungssektor und insbesondere die entsprechenden Verbände aufgerufen, umfassende, verbindliche und nachprüfbare Selbstverpflichtungen für eine datenschutzfreundliche Ausgestaltung der RFID-Technologie abzugeben.

Für den Schutz der Persönlichkeitsrechte der betroffenen Verbraucherinnen und Verbraucher sind dabei folgende Regeln unabdingbar:

Transparenz/Benachrichtigungspflicht

Die Verbraucherinnen und Verbraucher müssen wegen des möglichen Personenbezugs der auf RFID-Chips gespeicherten Daten umfassend über den Einsatz, Verarbeitungs- und Verwendungszweck und Inhalt von RFID-Chips informiert werden. Werden durch ihren Einsatz personenbezogene Daten gespeichert, sind die Betroffenen hiervon zu benachrichtigen.

Kennzeichnungspflicht

Nicht nur die eingesetzten RFID-Chips selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips, Lesegeräte bzw. dazugehörige Hintergrundsysteme ausgelöst werden, müssen für die Verbraucherinnen und Verbraucher transparent und leicht zu erkennen sein. Eine heimliche Anwendung „hinter dem Rücken" der Betroffenen darf es nicht geben.

Deaktivierung

Den betroffenen Verbrauchern muss ab dem Kauf von mit RFID-Chips versehenen Produkten die Möglichkeit eröffnet werden, die RFID-Chips jederzeit dauerhaft zu deaktivieren bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die ursprünglichen Speicherzwecke nicht mehr erforderlich sind. Dieses Recht darf nicht durch Gewährleistungsbeschränkungen in Allgemeinen Geschäftsbedingungen beeinträchtigt werden.

Datensicherheit

Die Vertraulichkeit der gespeicherten und der übertragenen Daten ist durch Sicherstellen der Authentizität der beteiligten Geräte (Peripherie) und durch Verschlüsselung zu gewährleisten. Das unbefugte Auslesen der gespeicherten Daten muss wirksam verhindert werden.

Keine heimliche Profilbildung

Daten von RFID-Chips aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Einwilligung der Betroffenen erstellt werden können.

Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Chips verzichtet werden.

21. Datenschutz international

21.1 Datenschutz bei Suchmaschinen

(Entschließung der 28. Internationalen Konferenz der Datenschutzbeauftragten London, Vereinigtes Königreich, am 2. und 3. November 2006)

Übersetzung aus dem Englischen

Vorgeschlagen von: Berliner Beauftragter für Datenschutz und Informationsfreiheit, Deutschland

Unterstützer: Deutschland (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit), Irland (Datenschutzbeauftragter), Neuseeland (Datenschutzbeauftragter), Norwegen (Datatilsynet), Polen (Generalinspektor für den Schutz personenbezogener Daten)

Heutzutage sind Suchmaschinen der Schlüssel zum „cyberspace" geworden, um in der Lage zu sein, Informationen im Internet aufzufinden, und damit ein unverzichtbares Werkzeug.

Die steigende Bedeutung von Suchmaschinen für das Auffinden von Informationen im Internet führt zunehmend zu erheblichen Gefährdungen der Privatsphäre der Nutzer solcher Suchmaschinen.

Anbieter von Suchmaschinen haben die Möglichkeit, detaillierte Interessenprofile ihrer Nutzer aufzuzeichnen. Viele IP-Protokolldaten, besonders wenn sie mit den entsprechenden Daten kombiniert werden, die bei Zugangsdiensteanbietern gespeichert sind, erlauben die Identifikation von Nutzern. Da die Nutzung von Suchmaschinen heute unter den Internet-Nutzern eine gängige Praxis ist, erlauben die bei den Anbietern populärer Suchmaschinen gespeicherten Verkehrsdaten, ein detailliertes Profil von Interessen, Ansichten und Aktivitäten über verschiedene Sektoren hinweg zu erstellen (z. B. Berufsleben, Freizeit, aber auch über besonders sensitive Daten, z. B. politische Ansichten, religiöse Bekenntnisse, oder sogar sexuelle Präferenzen).

Die Datenschutzbeauftragten sind bereits in der Vergangenheit hinsichtlich der Möglichkeit zur Erstellung von Profilen über Bürger besorgt gewesen. Die im Internet verfügbare Technologie macht diese Praxis jetzt in einem gewissen Umfang auf globaler Ebene technisch möglich.

Diese Entschließung bezieht sich nicht auf Suchfunktionen, die von Inhalteanbietern für ihre eigenen Angebote angeboten werden. Für den Zweck dieser Entschließung wird „Suchmaschine" definiert als ein Service zum Auffinden von Ressourcen im Internet über verschiedene Websites hinweg und basierend auf nutzerdefinierten Suchbegriffen.

Diese Entschließung betrifft nicht Probleme, die durch die Praxis vieler Betreiber von Suchmaschinen aufgeworfen werden, Kopien des Inhalts von Internetseiten einschließlich darauf enthaltener personenbezogener Daten, die dort legal oder illegal veröffentlicht werden, zu speichern und zu veröffentlichen („caching").

Vgl. z. B. den gemeinsamen Standpunkt zu Datenschutz und Suchmaschinen (zuerst verabschiedet auf der 23. Sitzung in Hongkong SAR, China ,15. April 1998, überarbeitet und aktualisiert bei der 39. Sitzung, 6. – 7. April 2006, Washington D. C.) der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation; http://www.datenschutz-berlin.de/doc/int/iwgdpt/search_engines_de.pdf. Vgl. ebenfalls Kapitel 5: „Surfen und Suchen" des Arbeitsdokuments der Artikel-29-Gruppe „Privatsphäre im Internet" – ein integrierter EU-Ansatz zum Online-Datenschutz; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpddocs/2000/wp37de.pdf.

Es ist offensichtlich, dass diese Informationen unter Umständen auf einzelne Personen zurückgeführt werden können. Deswegen sind sie nicht nur für die Betreiber von Suchmaschinen selbst von Nutzen, sondern auch für Dritte. So hat zum Beispiel vor kurzem ein Ereignis das Interesse unterstrichen, dass Strafverfolgungsbehörden an diesen Daten haben: Im Frühjahr 2006 forderte das Justizministerium

der Vereinigten Staaten von Amerika von Google, Inc. die Herausgabe von Millionen von Suchanfragen für ein Gerichtsverfahren, das unter anderem den Schutz vor der Verbreitung von kinderpornographischen Inhalten im Internet zum Gegenstand hatte. Google weigerte sich, dieser Aufforderung nachzukommen und gewann letztendlich das Verfahren. Im weiteren Verlauf desselben Jahres publizierte AOL eine Liste von beinahe 20 Millionen scheinbar anonymisierten Suchanfragen, die ungefähr 650.000 AOL-Nutzer über einen Zeitraum von drei Monaten in die AOL-Suchmaschine eingegeben hatten. Laut Presseberichten konnten daraus einzelne Nutzer auf der Basis des Inhalts ihrer kombinierten Suchanfragen identifiziert werden. Diese Liste war – obwohl sie von AOL umgehend zurückgezogen wurde, als der Fehler dort erkannt worden war – zum Zeitpunkt des Zurückziehens Berichten zufolge bereits vielfach heruntergeladen und neu publiziert, und in durchsuchbarer Form auf einer Anzahl von Websites verfügbar gemacht worden.

Es muss darauf hingewiesen werden, dass nicht nur die Verkehrsdaten, sondern auch der Inhalt von Suchanfragen personenbezogene Informationen darstellen können.

Diese Entwicklung unterstreicht, dass Daten über zurückliegende Suchvorgänge, die von Anbietern von Suchmaschinen gespeichert werden, bereits jetzt in vielen Fällen personenbezogene Daten darstellen können. Insbesondere in Fällen, in denen Anbieter von Suchmaschinen gleichzeitig auch andere Dienste anbieten, die zu einer Identifikation des Einzelnen führen (z. B. E-Mail), können Verkehrs- und Inhaltsdaten über Suchanfragen mit anderen personenbezogenen Informationen kombiniert werden, gewonnen aus diesen anderen Diensten innerhalb derselben Sitzung (z. B. auf der Basis des Vergleichs von IP-Adressen). Der Prozentsatz von Daten über Suchanfragen, die auf Einzelpersonen zurückgeführt werden können, wird vermutlich in der Zukunft weiter ansteigen wegen der Zunahme der Nutzung fester IP-Nummern in Hochgeschwindigkeits-DSL oder anderen Breitbandverbindungen, bei denen die Computer der Nutzer ständig mit dem Netz verbunden sind. Er wird noch weiter ansteigen, sobald die Einführung von Ipv6 abgeschlossen ist.

Empfehlungen

Die Internationale Konferenz fordert die Anbieter von Suchmaschinen auf, die grundlegenden Regeln des Datenschutzes zu respektieren, wie sie in der nationalen Gesetzgebung vieler Länder sowie auch in internationalen Richtlinien und Verträgen (z. B. den Richtlinien der Vereinten Nationen und der OECD zum Datenschutz, der Konvention 108 des Europarates, dem APEC Regelungsrahmen zum Datenschutz und den Datenschutzrichtlinien der Europäischen Union) niedergelegt sind, und gegebenenfalls ihre Praktiken entsprechend zu ändern:

1. Unter anderem sollten Anbieter von Suchmaschinen ihre Nutzer im Vorhinein in transparenter Weise über die Verarbeitung von Daten bei der Nutzung der jeweiligen Dienste informieren.

2. Im Hinblick auf die Sensitivität der Spuren, die Nutzer bei der Nutzung von Suchmaschinen hinterlassen, sollten Anbieter von Suchmaschinen ihre Dienste in einer datenschutzfreundlichen Art und Weise anbieten. Insbesondere sollten sie keine Informationen über eine Suche, die Nutzern von Suchmaschinen zugeordnet werden können, oder über die Nutzer von Suchmaschinen selbst aufzeichnen. Nach dem Ende eines Suchvorgangs sollten keine Daten, die auf einen einzelnen Nutzer zurückgeführt werden können, gespeichert bleiben, außer der Nutzer hat seine ausdrückliche, informierte Einwilligung dazu gegeben, Daten, für die Erbringung eines Dienstes die notwendig sind, speichern zu lassen (z. B. zur Nutzung für spätere Suchvorgänge).

3. In jedem Fall kommt der Datenminimierung eine zentrale Bedeutung zu. Eine solche Praxis würde sich auch zugunsten der Anbieter von Suchmaschinen auswirken, indem die zu treffenden Vorkehrungen bei Forderungen nach der Herausgabe nutzerspezifischer Informationen durch Dritte vereinfacht würden.

Für den Zweck dieser Erklärung bedeutet „Dritter" jede natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle außer der betroffenen Person, dem für die Verarbeitung Verantwortliche, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsdatenverarbeiters befugt sind, die Daten zu verarbeiten.

22. Anhang

22.1 Pressespiegel

Datum	Zeitung	Titel/Inhalt
11.01.2006	Nordsee-Zeitung	**„Daten-Speichern kappt Grundrecht“**
18.01.2006	Bild-Bremen	**Videos auf Discomeile**
26.01.2006	Bremer Tageszeitungen	**Jeder siebte Bremer steht in der Kreide** Nur Berlin schneidet laut Schuldneratlas schlechter ab
27.01.2006	Bremer Tageszeitungen	**Scoring – der Bürger wird durchleuchtet** Bewertungspunkte entscheiden über Kreditwürdigkeit
03.03.2006	Bremer Tageszeitungen	**Datenschutz für Handy und PC** Verfassungsrichter engen Zugriff auf gespeicherte Kontaktinformationen stark ein
04.03.2006	Bremer Tageszeitungen	**EU-Richtlinie ausgebremst?** Karlsruher Urteil gegen Handy- und PC-Überwachung kann Datenerfassung stoppen
08.03.2006	Kreiszeitung Syke	**Bald Videokameras auf den Fluren?** Misshandlung eines Bremer Häftlings gibt weiter Rätsel auf
08.03.2006	Bremer Tageszeitungen	**Lauschangriff muss noch mal vor Gericht** Kläger: Neufassung missachtet Karlsruher Auflagen
17.03.2006	Bremer Tageszeitungen	**Lagebild oder nur Powerpoint-Folien?** Grüne fordern mehr Informationen
17.03.2006	taz-nord-bremen	**Neue VS-Gesetze**
24.03.2006	Bremer Tageszeitungen	**Parlament beklagt zunehmenden Daten-Durst** Debatte über Bericht des Landesbeauftragten/Kritik an fehlendem Konzept im Bürger-Service-Center
31.03.2006	Nordsee-Zeitung	**Datenschützer kritisieren die Fußball-WM**
01.04.2006	Bremer Tageszeitungen	**BND überprüft auch Würstchenverkäufer** Datenschützer kritisiert Durchleuchtung in WM-Stadien
01.04.2006	taz-nord-bremen	**Wer ALG II bezieht, bekommt laut Bremens Datenschutzbeauftragtem weniger Rechte zugestanden**
02.04.2006	Bremer Tageszeitungen	**Bürgerrechte immer mehr eingeschränkt** Kritik des Bremer LfD im Jahresbericht
19.04.2006	Bremer Tageszeitungen	**Nachbesserungen beim Kleingedruckten** Teilnehmer von „Mit dem Rad zur Arbeit“ sauer über späteren Werbeanruf/Formulierung abgeändert
20.04.2006	Stern	**Versandhandel: Fragwürdige Anrufe** Bedenken des Bremer Datenschutzbeauftragten gegen das telefonische Mahnverfahren
04.05.2006	Weser-Report	**Pro & Contra** Gen-Erfassung von Hooligans?
24.05.2006	Bremer Tageszeitungen	**Fesseln für die Rasterfahndung** Bundesverfassungsgericht: Massenhafte Datensammlung kollidiert mit Grundgesetz
24.05.2006	taz-nord-bremen	**Bremens Politik auf dem falschen Fuß erwischt** Wie Bremen am 12. September 2001 die Rasterfahndung abschaffte, und innerhalb von sechs Wochen zurückruderte

Datum	Zeitung	Titel/Inhalt
24.05.2006	taz-nord-bremen	**Lauter neue Polizeigesetze** Nach dem Rasterfahndungsurteil des Bundesverfassungsgerichts muss Hamburg sein neues Polizeigesetz überarbeiten – und auch die anderen Nordländer müssen ihre bisherige Praxis ändern. Sie tun dies widerwillig.
24.05.2006	taz-nord-bremen	**Bremer Polizeigesetz verfassungswidrig** Auch die Bremer Rasterfahndung 2001/2002 hätte nach den Kriterien des Verfassungsgerichtes nicht sein dürfen
26.05.2006	Bremer Tageszeitungen	**Leistungsbescheide an Falschen geschickt** BagIS in der Kritik: Schlamperei beim Datenschutz
08.06.2006	Bremer Tageszeitungen	**Einig über neuen Datenschützer in Niedersachsen** SPD-Mann Hans-Joachim Wahlbrink wird Neddens Nachfolger
08.06.2006	Bremer Tageszeitungen	**Sicherheitslücken auf der Spur** Bremerhavener datenschutz nord GmbH wächst seit ihrer Gründung vor fünf Jahren stetig
02.12.2006	Bremer Tageszeitungen	**Datenautobahn für Amtsschimmel** Bremen übernimmt Federführung für einheitliche Standards bei der Datenübermittlung zwischen Bürgern, Behörden und Betrieben via Internet
14.07.2006	Kreiszeitung Syke	**Einblicke in die Stadtentwicklung** Recherche im Internet: Als erstes Bundesland hat Bremen eine umfassende Denkmaldatenbank
14.07.2006	Delmenhorster Kreisblatt	**Alle Bremer Denkmäler jetzt in einer Datenbank** Bremen ist damit Vorreiter in der Bundesrepublik
14.07.2006	taz-nord-bremen	**Alle Denkmäler auf einen Klick** Bundesweit führend: Bremens Denkmalamt stellt vollständige Datenbank online
09.07.2006	Bremer Tageszeitungen	**Big Brother bis du** Für einen Londoner Lokalsender übertragen Überwachungskameras jetzt direkt in die heimischen Wohnzimmer
22.09.2006	Nordsee-Zeitung	**Big Brother auf der Baustelle** Gewerkschaft verärgert über Webcams – „Arbeiter werden kontrolliert" – Unverständnis bei der Bean
04.10.2006	Bremer Tageszeitungen	**Bremer Bildungspolitiker stellen sich gegen die Kultusminister und lehnen ein Schüler-Datenregister ab** „Nicht jeden Blödsinn jahrelang speichern"
04.10.2006	Kreiszeitung Syke	**Grüne gegen KMK-Pläne**
22.12.2006	taz-nord-bremen	**Pausenhof-Überwachung macht Schule** Nach Hamburg und Niedersachsen führt auch erste schleswig-holsteinische Schule eine Pausenhof-Videoüberwachung ein. Auslöser waren gewalttätige Auseinandersetzungen zwischen Schülern und Attacken auf Lehrer
Dezember 2006	Bremer Tageszeitungen	**Untersuchungsausschusss „Kevin"** **Arzt aus dem Klinikum beruft sich auf Schweigepflicht** Vermeintlicher Vater Bernd K. lässt Erklärung verlesen

22.2 Telefonische Anfragen

Thema	Antragsteller/-in
Verletzung des Persönlichkeitsrechts durch Filmaufaufnahmen	Bürger
Fragen zu Auskunfteien	Mitarbeiterin einer Gesellschaft
Auskünfte des Standesamtes zum Zweck der Ahnenforschung	Bürger
Schadensersatzanspruch aus § 8 BDSG, § 823 BGB, Höhe des Anspruches	öffentliche Stelle
Beschlagnahme von Datenträgern eines Apothekers durch die Polizei Bremen	externer betrieblicher DSB
Fragen zur SCHUFA-Klausel und -Selbstauskunft	Bürgerin
Fragen zur Bestellpflicht, Anwendbarkeit des BDSG auf Rechtsanwälte, Bestellmöglichkeit von externen DSB's, Kontrollkompetenz des LfDI, anlassunabhängige Kontrolle?	Steuerberater/ Rechtsanwalt
Beschwerde über Gebührenbefreiung bei der GEZ	Bürger
Fragen zu einer Werbemailing-Aktion der Post	Apotheker
Beschwerde über Datensicherheit bei einem Provider	Kunde
Voraussetzungen für eine Telefonüberwachung, Benachrichtigungspflicht	Bürger
Kann sich ein indisches Unternehmen auf die Safe-Harbor-Liste setzen lassen?	Konzern
Darf die Polizei bei einer Krankenkasse zur Beweisgewinnung Rezepte beschlagnahmen?	Bürgerin
Darf ein Rechtsanwalt Unternehmen anschreiben und fragen, ob sich die gegnerische Partei in einem Scheidungsverfahren bei diesen beworben hat?	Bürgerin
Fragen zu Forschungsvorhaben	Wissenschaftlerin
Datenübermittlung der Polizei an das Amt für Soziale Dienste	Bürgerin
Fehlversendung durch das Job Center	Bürgerin
Weitergabe von Gesundheitsdaten an Abrechnungsstelle ohne Einwilligung	Bürgerin
Frage zur rechtlichen Bedeutung von E-Mail „Disclaimern“	behördlicher DSB
Darf eine Hausverwaltungsfirma Fotos vom Innenbereich einer Mietwohnung machen?	Mieter
Bekanntgabe nichtanonymisierter Daten von Einwendern im Bauverfahren	behördlicher DSB
Datenerhebung unter Hypnose	Bürgerin
Übermittlung von Personaldaten durch ein Unternehmen	Bürger
Einsichtnahme in Personalakten durch die Kripo	behördlicher DSB
Zulässigkeit von Werbesendungen	betrieblicher BSB
Inhalt von Mitarbeiterbeurteilungen	Personalrat
Auskunft aus Personenstandsbüchern	Bürger
Weitergabe von Kreditdaten durch eine Bank an einen Hauskäufer	Bürgerin
Schutz von Sozialdaten	Bürger

Thema	Antragsteller/-in
Fragen zum Mikrozensus	Bürger
Verschlüsselung von E-Mails durch öffentliche Stelle	Behörde
Akteneinsichtsrecht gegenüber Staatsanwaltschaft	Bürger
Übermittlung von Bestands- und Verbindungsdaten aus Telekommunikation an die Polizei	betrieblicher DSB
Doppelter Stempel auf dem Rundfunkgebührenbefreiungsantrag erforderlich	Sozialverein
Datenerhebung durch Auskunftei	Bürgerin
Erhebung von Daten für die Dienstleistungsstatistik	Bürger
Veröffentlichung personenbezogener Daten auf einer Homepage	Bürgerin
Personalausweiskopien durch Telekommunikations-Diensteanbieter	Bürger
Wer übermittelt Daten an die GEZ?	Bürger
Auslegung des Bundesdatenschutzgesetzes	Behörde
Fingerabdruckerfassung bei Packstationen der Deutschen Post	Bürger
Veröffentlichung falscher Daten unter Google	Bürger
Verarbeitung personenbezogener Daten durch ein Lotterieunternehmen	Bürger
Zulässigkeit der Auftragsdatenverarbeitung bei Patientendaten	betrieblicher DSB
Löschung von Daten bei der Polizei	Bürger
Angabe personenbezogener Daten bei Nebentätigkeitsgenehmigung	externer behördlicher DSB
Verfahrensverzeichnis für ein Rechtsanwaltsbüro	Anwalt
Führung von Adressdateien	Bürger
Verfolgungsbehörde bei Ordnungswidrigkeiten nach dem BremDSG	behördlicher DSB
Erhebung von Daten durch eine Reiserücktrittsversicherung	Bürgerin
Erhebung von Daten durch ein Versandhandelsunternehmen	Bürger
Löschungsfristen der SCHUFA	Bürger
Nutzung personenbezogener Daten durch Rettungsdienstleister zur Eigenwerbung	Behörde
Auskunft über personenbezogene Daten bei der Polizei Bremen	Bürger
Betriebsvereinbarung Internetnutzung	betrieblicher DSB
Erhebung von Daten durch Auskunfteien	Bürger
Durchführung von Evaluationen an Hochschulen	Hochschule
Erhebung von Betriebsdaten zu Controlling-Zwecken	Beschäftigte
Sicherheit beim Transport von Gesundheitsdaten von einem externen Labor an den Betriebsarzt	Beschäftigte
Mitnahme von Patientendaten/-unterlagen durch einen Krankenhausarzt bei Eröffnung einer Praxis auf dem Krankenhausgelände	Patienten

Thema	Antragsteller/-in
Sichere Vernichtung von sensiblen Bons durch Apotheken	betrieblicher DSB
Forschungsvorhaben an der Uni Bremen	Eltern und Schüler
Outsourcing der Poststelle eines Unternehmens	Fahrgäste und Arbeitnehmer
Woher erhält die GEZ Mitarbeiterdaten?	Betroffener
Vorlage einer Bescheinigung des Vermieters über die Berechtigung des Mieters zur Untervermietung	ALG-II-Antragsteller, Vermieter und Mieter
E-Mail und Internet für Schweigepflichtige	EDV-Leiter
Auskünfte aus dem Familienbuch	
Datenschutz bei der Bremischen Evangelischen Kirche	Behörde
Datenschutz und Datenabgleich bei der BAgIS	Bürger
Ist die Verlesung eines PKH-Antrages bei Gericht zulässig?	Bürgerin
Veröffentlichung von personenbezogenen Daten im Internet ohne Einwilligung	Bürger
Zulässigkeit der Veröffentlichung von Geburtstagen durch eine Partei	Mitgliederverwaltung
Korrektur falscher Daten in einem Strafverfahren	Betroffener
Legitimationsprüfung der Spadaka durch Kopie des Personalausweises	Kontobevollmächtigte
Datenschutz im DV-Unternehmen	Unternehmen
Videoüberwachung auf Baustellen	Bauarbeiter
Auskunftsansprüche des Betroffenen	Bürger
Verbleib von Patientenakten verstorbener Ärzte	Patienten
Anruf vom CallCenter	Energieprotestler
Speicherung von Daten Minderjähriger bei der Polizei Bremen	Bürger
Missbrauch des Einsichtsrechts in Grundbuch durch Notariat	Bürger
Übermittlung von Grundsteuerdaten an Katasteramt	Grundsteuerzahler
Offenbarung von Gesundheitsdaten bei Verkauf eines Laptops	Heimbewohner
Verarbeitung des Datums „Nationalität“ für Dienstreisen	Mitarbeiter von Kunden Dienstreisebüros
Auskunft der Polizei über Verantwortliche eines insolventen Reisebüros	Behörde
Kenntlichmachung von Videoüberwachungskameras auf Campingplatz	Inhaberin/Platzwart
Internetdatenbank mit allen in Bremen ansässigen Ärzten	Bürger
Videoüberwachung in einem Büroraum mit Kundenverkehr	Arbeitnehmer und Kunden
Einsichtnahme über Deckspiegel in Pinpad bei einem Supermarkt	Kunde
Auf der Krankenversichertenkarte gespeicherte Daten	Versicherter
Datenerhebung von Steuerberatern bei Ärzten – Schweigepflichtsentbindung	externer betrieblicher DSB

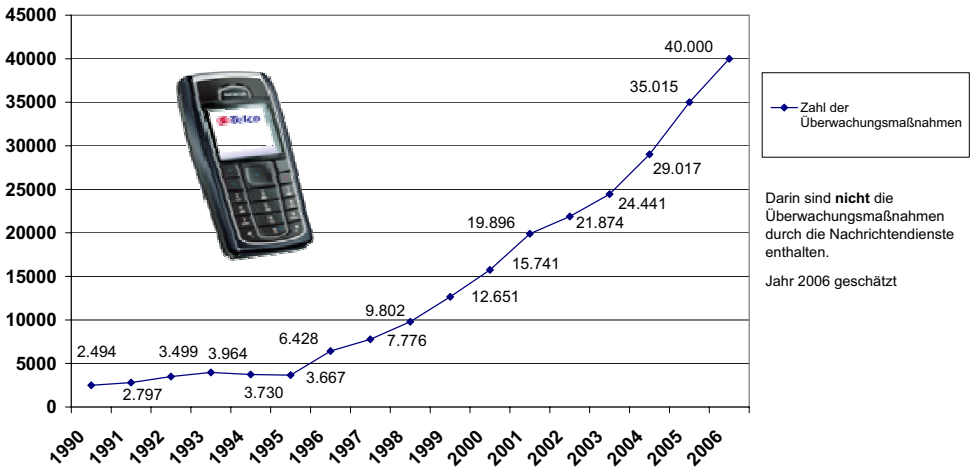
Thema	Antragsteller/-in
Löschung von Daten (inkl. Gesundheitsdaten) über Spenden	Haftinsassen
Speicherung von Daten durch die Polizei Bremen bei Personenkontrolle	Bürger
Verarbeitung von Schülerdaten	Lehrerin
Nachweis einer eheähnlichen Gemeinschaft bei Antrag auf ALG II	Betroffener
Arten von gespeicherten Daten auf der elektronischen Gesundheitskarte	Bürger
Whistleblowing – Bearbeitungssachstand im Düsseldorfer Kreis (vom BfDI an uns verwiesen)	Rechtsreferendar Ffm.
Datengeheimnis im Heim für Ergotherapie	Heimangestellte
Verschwiegenheitsverpflichtung von Mitarbeitern	öffentliche Stelle
Datenschutz in Parteien, Bestellpflicht eines DSB für Fraktionen	Partei
Arbeitnehmerüberwachung bei der Bildschirmarbeit	Arbeitnehmer
Datenverarbeitung bei der Familienkasse	Bürger
Auftragsdatenverarbeitung bei Steuerberaterkanzlei	Bürger
Fragen zum Informationsregister (IFG)	Behörde
Darf ein Klassenbuch öffentlich ausgelegt werden?	Schule
Polizeiliche Auskunft an Landkreis	Behörde
Erhebung von Gesundheitsdaten durch ein Raucherentwöhnungsinstitut	Institutsangehöriger
Aufzeichnung von Telefongesprächen bei Behörden	behördlicher DSB
Probleme bei der Gebührenbefreiung mit der GEZ	Bürger
Weiterleitung von Telefongesprächen und E-Mails auf eine andere Firma ohne Einwilligung der Firmenleitung	Geschäftsleitung
Zusammenfassung von IGLU-Ergebnissen mit Schulinspektorenberichten	Lehrkräfte
Findet § 28 BDSG Anwendung auf Datenschutz in Vereinen?	Verein
Benachrichtigung des Betr. nach § 33 zweier Auskunfteien in einem Brief	Kundin
Vernichtung von Gesundheitsakten verstorbener ehemaliger Vulkanesen	Arbeitnehmer
Auskünfte der Meldebehörde	Bürger
Schulung für betriebliche DSB	Angestellter einer Firma
Wartung DV-Anlagen durch Externe	DSM/Direktor und Personalrat
Geltung des § 40 BDSG auch für nicht öffentliche Forschungslabors	Arbeitnehmer
Verwendung von Gutachten beim psychologischen Dienst der BA	Kunde
Adressenanforderung von Parteien bei Meldebehörden	Bürger
Telefonische Verkaufsverhandlungen erlaubt?	Bürger
Aushang einer Liste über Schwerbehinderte zur Wahl der Schwerbehindertenvertretung	Schwerbehinderte

Thema	Antragsteller/-in
Adressenänderung von Meldebehörde an die GEZ	Bürger
Weitergabe persönlicher Angaben der Mutter eines Patienten an den Kinderarzt durch den Kinderpsychologen	Mutter und Patient
Vorlage von Kontoauszügen sowie Angabe der Kranken- und Rentenversicherungsnummer an die BAgIS	ALG-II-Antragsteller
Aufbewahrungsfristen in der Verwaltung	Rechtsanwaltskanzlei
Durchsuchen von Mülltonnen durch einen Nachbarn	Nachbarn
Erhebung und Speicherung von Lehrer- und Schülerdaten zur Einhaltung des Rauchverbots in Schulen	Lehrer, Schüler
Einsichtnahmemöglichkeit einer Bausparkasse in das Grundbuch	Bürgerin
Gesicherte Aufbewahrung zu archivierender Unterlagen	Unternehmen
Abnahme von Fingerabdrücken bei Verkehrskontrolle	Bürger
Erteilung von Auskünften an den Betroffenen durch eine Auskunftei	Bürger
Löschung von personenbezogenen Daten beim Verfassungsschutz	Bürger
Umfang der Erhebung von Daten durch das Finanzamt	Bürger
Veröffentlichung des beruflichen Werdegangs eines Hochschullehrers im Internet	Hochschullehrer bzw. Beschäftigter
Verwendung von Fahrtenbuchaufzeichnungen zur Kosten- und Leistungsrechnung	Beschäftigte
Auskunftspflicht des Arbeitgebers gegenüber dem Sozialamt	Sozialhilfeempfänger einer Behindertenwerkstatt
Bestellung eines Datenschutzbeauftragten	Behörde
Verfahren zur Auswahl der teilnehmenden Apotheken und Versicherten für den Testbetrieb der elektronischen Gesundheitskarte	Redakteur Ärztezeitung
Blutentnahme durch den Betriebsarzt ohne Angabe des Zweckes	Arbeitnehmer
Aufbau einer Netzstruktur mit Zugriff auf alle Daten	Arbeitnehmer
Rückschluss auf einen Schüler durch die lD-Nummer im Rahmen eines Forschungsvorhabens	Schüler
Ehrverletzungsdelikte im Internet durch Schüler	Lehrerin
Ausgliederung aus einer öffentlichen Stelle, Bestellpflicht eines DSB	neue nicht öffentliche Stelle
Darf sich die Telekom Personalausweis vorlegen lassen?	Bürger
Datenverarbeitung der BAgIS	Bürgerin
Forschungsvorhaben an der Uni Bremen	Schüler
Vorhalt der Kontonummer durch Werbeunternehmen	Bürgerin
Erhalt von Telefonrechnungen mit Auflistung einer anderen Person	Bürgerin
Videoüberwachung auf einem Privatgrundstück	Unbefugte Personen
Aufzeichnen und Mithören von Telefongesprächen im CallCenter	Beschäftigte, Kunden

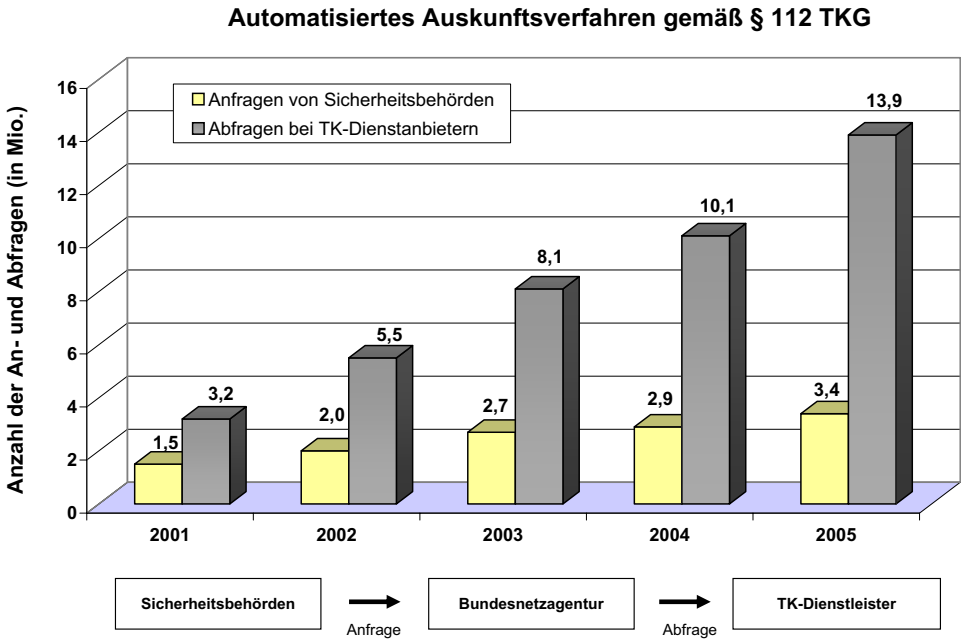
Thema	Antragsteller/-in
Zugriff auf Betriebsrat- und persönliche Daten durch den Arbeitgeber	Betriebsrat/ Arbeitnehmer
Fragen zum externen Datenschutzbeauftragten	Unternehmen
Datenerhebung beim bisherigen Hauseigentümer über den neuen Hauseigentümer durch die Entsorgungsbetriebe	Hauseigentümer als abfallüberlassungspflichtiger Gebührenzahler
Regelmäßige Vorlage der Verdienstbescheinigung gegenüber dem Vermieter	Mieter einer Sozialwohnung
Übermittlung von Diagnosedaten an die Polizei bei Verdacht auf Kindesmisshandlung	DSB einer Krankenkasse
Personaldaten an der Klingelanlage einer Behörde	Beschäftigte
Unbeschränkte Auskünfte aus dem Bundeszentralregister	Behörde
Veröffentlichung von Protokollen nicht-öffentlicher Beiratssitzungen	Behörde
Einsicht in Personalakten durch eine Praktikantin	Beschäftigte
Weitergabe von Mieterdaten an einen Dritten	Mieter
Videoüberwachung in einer Wohnanlage	Bewohner, Besucher, Handwerker etc.
Datenerhebung bei einem Wohnungsunternehmen durch die Polizei	Mieter
Aufnahme von Unterlagen über personelle Maßnahmen in die Personalakte	Beamte
Einsicht in die Nebenkostenabrechnung anderer Mieter	Mieter
Outsourcing der Personalabrechung	Beschäftigte
Vorlagepflicht bei Standardvertragsklauseln	Rechtsanwaltskanzlei
Verhaltens- und Leistungskontrollen bei Behörden	behördlicher DSB
IT-Sicherheitskonzept nach dem KontraG und der EuroSOX-RL	Bürger
Individuelle Verhaltenskontrolle	Beschäftigter
Einwilligungserklärung bei Verein	Bürger
Evaluierung von Lehrveranstaltungen	Hochschullehrer und Lehrbeauftragte
Wahrung des Fernmeldegeheimnis bei E-Mail-Verkehr während eines Sabbatjahres	Beschäftigter
Name, Telefon- und Zimmernummer an der Eingangstür	Beschäftigte
Nutzung von Krankenversichertendaten zu Werbezwecken	Krankenversicherte
Aufbewahrungsfrist für Bewerbungsunterlagen	Bewerber
Umfang der Datenerhebung bei einer Hausdurchsuchung	Beschuldigter
Austausch von Adressdaten über Angehörige einer Selbsthilfegruppe	Angehörige einer Selbsthilfegruppe
Ausweiskopie trotz hinterlegter Ausweisdaten durch Kreditinstitut	Bürgerin
Weitergabe von Krankheitsdaten an Dritte durch den Arbeitgeber	Beschäftigte

Thema	Antragsteller/-in
Einstellung des Wählerverzeichnisses für eine Betriebsratswahl in das Intranet	wahlberechtigte Beschäftigte
Weitergabe von Mietverträgen an Dritte durch Vermieter	Mieter
Angabe der Urlaubsanschrift auf dem Urlaubsantragsformular	Beschäftigte
Eintragung in Robinson-Liste	Bürger
Forschungsvorhaben mit Patienten eines Reha-Zentrums	Patienten
Mitteilung über eine einstellungshindernde Eintragung im polizeilichen Führungszeugnis an eine andere öffentliche Stelle	Bewerber für Kinder- und Jugendbetreuung
Regelungen über die Art und Weise der Löschung von Daten auf Datenträgern	Betroffene
Akteneinsichtsrecht gegenüber der BAgIS	ALG-II-Bezieher
Auskünfte aus dem Einwohnermelderegister	Bürgerin
Schutz von personenbezogenen Daten im Zeugenschutzprogramm	Behörde
Auskunft aus dem Bundeszentralregister	Bürger
Tragen von Schildern mit Vor- und Zunamen im Krankenhaus	Krankenschwester
Einhaltung von Auskunftssperren im Einwohnermelderegister	Bürger
Aufnahme von Angaben über die Schwangerschaft in einen Einsatzplan	Beschäftigte
Einsichtnahme in Ehescheidungsakte durch Gericht und Staatsanwaltschaft	Prozessbeteiligte

22.3 Anstieg der Telefonüberwachung



Die aktuellen Zahlen der tatsächlich in 2006 durchgeführten Maßnahmen der Telefonüberwachung liegen noch nicht vor. Meine im letzten Jahresbericht abgegebene Schätzung von 32.000 (vgl. 28. JB, Ziff. 21.3) wurde noch weit übertroffen.



Sicherheitsbehörden erhalten gemäß § 112 Telekommunikationsgesetz (TKG) über die Bundesnetzagentur von Telekommunikationsdienstanbietern Auskünfte aus deren Kundendateien (Namen und Anschrift der Inhaber von Rufnummern). Der Kreis der ins automatisierte Verfahren eingebundenen Behörden und verpflichteten Unternehmen wurde im Laufe der Jahre stetig vergrößert. Nach dem Jahresbericht der Bundesnetzagentur zu 2005 können ca. 1.000 bei der Reg TP registrierte Sicherheitsbehörden bei insgesamt 85 Telekommunikationsdienstanbietern entsprechende Bestandsdaten abfragen. Im abgebildeten Diagramm ist die Entwicklung beim automatisierten Auskunftsverfahren gemäß § 112 TKG im Zeitraum 2001 bis 2005 dargestellt.

22.4 Liste des verfügbaren Informationsmaterials

Informationen zu verschiedenen Bereichen können im Internet unter www.datenschutz.bremen.de abgerufen werden; hier gibt es auch Downloads für Formulare.

Folgende Informationsmaterialien können beim

Landesbeauftragten für Datenschutz und Informationsfreiheit
der Freien Hansestadt Bremen

Postfach 10 03 80 27503 Bremerhaven
Telefon: 04 71 / 9 24 61-0 Telefax: 04 71 / 9 24 61-31
E-mail: office@datenschutz.bremen.de

angefordert werden:

25. Jahresbericht 2002, Bürgerschafts-Drs. 15/1418 (Restexemplare)
26. Jahresbericht 2003, Bürgerschafts-Drs. 16/189 (Restexemplare)
27. Jahresbericht 2004, Bürgerschafts-Drs. 16/578 (Restexemplare)
28. Jahresbericht 2005, Bürgerschafts-Drs. 16/980 (Restexemplare)

Broschüre „Datenschutz bei WindowsNT“
Broschüre „Orientierungshilfe – Datenschutz bei Dokumentenmanagementsystemen“
Faltblatt „Das Informationsfreiheitsgesetz des Bundes“
Faltblatt „Datenschutz im Verein“
Faltblatt „Adressenhandel und unerwünschte Werbung“
Faltblatt „Handels- und Wirtschaftsauskunfteien“
Faltblatt „Hinweise zum Antrag Arbeitslosengeld II“
Faltblatt „Meine Datenschutzrechte als Telefonkunde“
Faltblatt „Keine Spione auf der Festplatte“

Faltblatt	„Verräterische Spuren auf Festplatten“
Faltblatt	„Videoüberwachung durch private Stellen“
Faltblatt	„Surfen am Arbeitsplatz – Datenschutz-Wegweiser“
BfD-Info 1	Bundesdatenschutzgesetz – Text und Erläuterungen –
BfD-Info 2	Der Bürger und seine Daten
BfD-Info 3	Schutz der Sozialdaten (zurzeit nicht verfügbar, Neuauflage ist geplant)
BfD-Info 4	Die Datenschutzbeauftragten in Behörde und Betrieb
BfD-Info 5	Datenschutz in der Telekommunikation (zurzeit nicht verfügbar, 6. Auflage wird überarbeitet)

Die Broschüren BfD-Info 1 bis 5 können beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit auf dessen Homepage (www.bfdi.bund.de) eingesehen und heruntergeladen werden.

22.5 Glossar

Abkürzung	Erklärung
A2LL	Verfahren zur Berechnung des Arbeitslosengeldes II
AD	Active Directory, bremischer Verzeichnisdienst
AfSD	Amt für Soziale Dienste
AFZ	Ausbildungsförderungszentrum im Land Bremen GmbH
AG	Arbeitsgruppe/Arbeitsgemeinschaft
AGB	Allgemeine Geschäftsbedingungen
AGG	Allgemeines Gleichstellungsgesetz
ALG II	Arbeitslosengeld II
AO	Abgabenordnung
ArbVG	Arbeitsvertragsgesetz
ARGE	Arbeitsgemeinschaft
Auditing	Gutachterliche Untersuchung eines DV-Verfahrens
Authentifizierung	Ausweisen für einen berechtigten Zugriff
AZE	Arbeitszeiterfassung
BA	Bundesagentur für Arbeit
BAföG	Bundesausbildungsförderungsgesetz
BAgIS	Bremer Arbeitsgemeinschaft für Integration und Soziales
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BfV	Bundesamt für Verfassungsschutz
BGBl.	Bundesgesetzblatt
BGH	Bundesgesetzhof
BIPS	Bremer Institut für Präventionsforschung und Sozialmedizin
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtsgesetz
BMWA	Bundesministerium für Wirtschaft und Arbeit (ehemaliges)
BR-Drs.	Bundesratsdrucksache
BreKom	Bremer Kommunikationstechnik
BremBG	Bremisches Beamtengesetz
BremDSG	Bremisches Datenschutzgesetz
Brem.GBl.	Bremisches Gesetzblatt
BremHG	Bremisches Hochschulgesetz
BremIFG	Bremer Informationsfreiheitsgesetz
BremKRG	Bremisches Krebsregistergesetz
BremMeldG	Bremisches Meldegesetz
BremPolG	Bremisches Polizeigesetz
BremSchulDSG	Bremisches Schuldatenschutzgesetz

Abkürzung	Erklärung
BremVerfSchG	Bremisches Verfassungsschutzgesetz
BremVwVfG	Bremisches Verwaltungsverfahrensgesetz
BSC	Bürger-Service-Center
BSI	Bundesamt für die Sicherheitstechnik
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVN	Bremer Verwaltungsnetz
BZR	Bundeszentralregister
Client	Beteiligung eines PC (Kunde) in einem Netzwerk
DFB	Deutscher Fußball-Bund
DMS	Dokumentenmanagementsystem
DMZ	Demilitarisierte Zone
DNA	Träger der Erbinformationen („Genetischer Code“) in Lebewesen
DOS	Betriebssystem
DSB	Datenschutzbeauftragter
DSL	Digital Subscriber Line, breitbandige digitale Verbindung über Telefonnetze
DV	Datenverarbeitung, auch Dienstvereinbarung
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
eGK	elektronische Gesundheitskarte
eGovernment	elektronische Verwaltung
Erfa-Kreis	Erfahrungskreis der Datenschutzbeauftragten
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EVGP	Elektronisches Verwaltungs- und Gerichtspostfach
FahrlG	Fahrlehrergesetz
FahrlGDV	Durchführungsverordnung zum Fahrlehrergesetz
Firewall	Programm zum Schutz von Angriffen aus dem Internet
GDD	Gesellschaft für Datenschutz und Datensicherung e. V.
GDV	Gesamtverband der deutschen Versicherungswirtschaft
GEZ	Gebühreneinzugszentrale
GPS	Global Positioning System
HandwO	Handwerksordnung
HBH	Hansestadt Bremisches Hafenamt
HGB	Handelsgesetzbuch
Homepage	Eingangs- und Eröffnungsseite einer Internetadresse
http	Hypertext Transfer Protocol, Protokoll zur Übertragung von Daten in einem Netzwerk
iBON	Integratives Bremer Onkologie- und Hämatologie Netzwerk
ID	Identität
ID Bremen GmbH	Informations- und Datentechnik Bremen GmbH
IGLU	Internationale Grundschul-Lese-Untersuchung
IHK	Industrie- und Handelskammer
IMEI	International Mobile Equipment Identity (Handy)
IMSI	International Mobile Subscriber Identity (Handy)
INPOL	Polizeiliches Informationssystem
IP	Internet Protocol
ISAWeb	Informationssystem Sachen und Anzeigen im Polizeinetz
ISDN	Integrated Services Digital Network (das digitale Telefonnetz)
IT	Informationstechnologie

Abkürzung	Erklärung
IuK	Informations- und Kommunikationstechnologien
JB	Jahresbericht
Kfz	Kraftfahrzeug
KpS	Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen
KMK	Kultusministerkonferenz
LAN	Local Area Network (lokales Netzwerk)
LfDI	Landesbeauftragter für Datenschutz und Informationsfreiheit
LfV	Landesamt für Verfassungsschutz
LKA	Landeskriminalamt
LUNA	Länderumfassende Namensabfrage
MAGELLAN	Schulverwaltungssoftware
MeldDÜV	Meldedatenübermittlungsverordnung
MESO	Meldebehördensoftware
MiP	Mitarbeiterportal
OSCI	Online Services Computer Interface, sichere und vertrauliche Übertragung digital signierter Dokumente über das Internet
OU	Organisationseinheiten
PAVwV	Verwaltungsvorschrift über die Erhebung und Führung von Personalaktendaten
PC	Personalcomputer
PDA	Personal Digital Assistant (elektronisches Notizbuch)
PHW	Personengebundene Hinweise
PISA	Program for International Student Assessment
PsychKG	Gesetz über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten
Pull-Verfahren	Abrufverfahren
PuMa	Personalverwaltung und -management
RFID	Radio Frequency Idendification, Funk-Erkennung
RGbStV	Rundfunkgebührenstaatsvertrag
RL	Richtlinie
Router	Gerät, zum Steuern von Datenpaketen im Netz
RTP	Real Time Transport Protocol, Protokoll zur kontinuierlichen Übertragung von audiovisuellen Daten über IP-basierte Netzwerke
SCHUFA	Schutzgemeinschaft des kreditgewährenden Gewerbes
Scoring	Bewertung
Security-Gateway	Rechner, der Daten- bzw. Rechnernetze sicher verbindet
Server	ist ein Computer in einem Netzwerk, der andere Computer bedient
SfJuV	Senator für Justiz und Verfassung
SGB	Sozialgesetzbuch
SHA	Secure Hash Algorithm
Signatur	elektronische Unterschrift
SIM-Karte	Speicherkarte (Handy)
SIP	Session Initiation Protocol, Protokoll zum Aufbau einer Kommunikationssitzung zwischen mindestens zwei Teilnehmern
SMS	Short Message Service, Kurznachrichten via Mobiltelefon
SSL	Security Socket Layer (Internet-Protokoll zur sicheren Datenübertragung
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz

Abkürzung	Erklärung
SÜG	Sicherheitsüberprüfungsgesetz
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TET	Trusted Execution Technology
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TOMs	Technisch-organisatorische Maßnahmen gem. § 7 BremDSG
TPM	Trusted Platform Module
TÜV	Technischer Überwachungsverein
UDS	Unfalldatenspeicher
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
USB	Universal Serial Bus, standardisierte Steckverbindung
VMZ	Verkehrsmanagementzentrale
VoIP	Voice over Internet Protocol, Telefonieren über Computernetzwerke auf der Basis des IP-Protokolls
VPN	Virtual Private Network
VPN-Tunnel	Virtual Privat Networking, abgesicherter Datenstrom
VPS	Virtuelle Poststelle
WLAN	Wireless Local Area Network (Funknetz)
WVO	Werkstättenverordnung
Ziff.	Ziffer
ZKA	Zentraler Kreditausschuss der deutschen Kreditwirtschaft
ZSS	Zentrale Speicherstelle

22.6 Index

Druck: Anker-Druck Bremen