30. Jahresbericht

des Landesbeauftragten für Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats über das Ergebnis der Tätigkeit im Jahre 2007 den 30. Jahresbericht zum 31. März 2008 (§ 33 Abs. 1 Bremisches Datenschutzgesetz – BremDSG). Redaktionsschluss für die Beiträge war der 31. Dezember 2007.

Sven Holst

Landesbeauftragter für Datenschutz und Informationsfreiheit

Inhaltsverzeichnis

1. Vorwort

1.1 Von den alten Ägyptern lernen

„Oh, ihr Lebenden! Ein Weiser ist der, der sich anhört, was die Vorfahren gesagt haben!“ Mit dieser Inschrift wandte sich vor Jahrtausenden der hohe ägyptische Beamte Rech-mi-Re an jene, die in Theben sein Grab besuchten. Diese Worte möchte man in Abwandlung auf das erst vor fast 25 Jahren verkündete Volkszählungsurteil des Bundesverfassungsgerichts an den Bundesinnenminister Schäuble richten. In das Urteil ist das Recht auf informationelle Selbstbestimmung „gemeißelt“. In der westlichen Welt kamen Zeiten, in denen die Besucher des Grabes die Inschrift nicht mehr lesen konnten. Das Wissen um die Bedeutung der Hieroglyphen war verloren gegangen. Es sollten fast 2000 Jahre verstreichen, bis die Inschrift wieder gelesen und verstanden werden konnte. Man kann nur hoffen, dass diese Leseschwäche nicht nur im Amte des Bundesinnenministers, sondern auch in anderen Bereichen der Politik in Bezug auf die verfassungsrechtlichen Grundsätze des Volkszählungsurteils schneller vorübergehen möge.

1.2 Mehr Respekt vor der Verfassung

In den letzten Jahren hat es in besonderem Maße eine ganze Reihe von Entscheidungen des Bundesverfassungsgerichts mit datenschutzrechtlicher Relevanz gegeben (vgl. Ziff. 9.9, 9.15 und 15.2 dieses Berichts). Die Gesetzgeber des Bundes und einiger Länder haben dabei oft erfahren müssen, dass sie das Recht auf informationelle Selbstbestimmung in ihren Gesetzen nicht ausreichend beachtet haben. Übrigens sind diese verfassungswidrigen Gesetze oft entgegen der Warnungen der Datenschutzbeauftragten des Bundes und der Länder verabschiedet worden. Dabei ist eine gewisse Erosion bei der Beachtung des Datenschutzes durch den Gesetzgeber festzustellen, denn viele der neu auf den Weg gebrachten gesetzlichen Regelungen mit Eingriffen in das informationelle Selbstbestimmungsrecht liegen nicht im verfassungsrechtlichen Rahmen. Bedauerlicherweise werden solche Gesetzentwürfe oft bei der Befassung im Bundesrat nicht kritisiert, vielmehr wird von hier mit Mehrheit versucht, die gesetzlichen Eingriffe noch zu verschärfen. Viele Bürgerinnen und Bürger, die sich mit einem Anliegen an mich wenden, fragen häufig vorab resignierend, ob ich denn in ihrer Angelegenheit überhaupt noch etwas tun könne. Ein Bürger brachte es mit den Worten auf den Punkt: „Ich habe nichts zu verbergen, aber ich habe das Gefühl, ich kann auch nichts mehr verbergen“. Das Vertrauen der Bürgerinnen und Bürger, dass der Staat mit ihren Daten respektvoll umgeht, ist im Schwinden, wie sonst ist z. B. die Flut der Anfragen bei mir im letzten Jahr zu erklären, bis wann man noch einen Ausweis ohne darin gespeicherte Fingerabdruckdaten beantragen könne.

1.3 Überreaktionen der Innenpolitik des Bundes

Der scheidende Bundeswirtschaftsminister Clement soll auf die Frage, was er jetzt mache, seinerzeit geantwortet haben: „Ich werde meine Freiheit genießen, soweit es Otto Schily zulässt“.

Gerade auf dem Feld der Innenpolitik kommen die öffentlich gemachten Ideen, die mit verfassungsrechtlich bedenklichen Eingriffen verbunden sind, in immer kürzeren zeitlichen Intervallen. Hatte schon der ehemalige Innenminister Schily erklärt, er habe mit seinen gesetzgeberischen Initiativen alles getan, um den Terrorismus in Deutschland zu verhindern, brachte Bundesinnenminister Schäuble es fertig, in nicht vorstellbarer Vielfalt die Ängste der Bürger vor Terrorismus und Kriminalität zu schüren. Ihm gelang es, europäische Gremien (vgl. Fluggastdatenabkommen mit den USA oder die Vorratsdatenspeicherung) wie auch die Mehrheit des Bundestages dazu zu bewegen, durch ein Klima der Verunsicherung alle Bundesbürger als potentielle Gefahrenquelle zu diskreditieren, der nur mit präventiven nachrichtendienstlichen und polizeilichen Mitteln permanenter Überwachung Einhalt geboten werden könne. Erneute massive Eingriffe in die Freiheitsrechte, insbesondere in das Recht auf informationelle Selbstbestimmung, waren die Folge.

Der frühere Bundesinnenminister Baum formulierte es so: "Wir sind auf einer Rutschbahn, in der ständig auf eine Ausnahmesituation mit Ausnahmegesetzen reagiert wird. Zur Logik des Sicherheitsstaates gehört die Maßlosigkeit“.

Erschreckend ist, wie dabei oft die Öffentlichkeit für dumm verkauft wird. Viele der vorgeschlagenen Maßnahmen sind gegen gut organisierte Terroristen wirkungslos. Sie treffen aber ins Herz einer freien Gesellschaft. Der Staat mischt sich immer mehr in alle Lebensbereiche seiner Bürger ein. Es gibt trotzdem keine absolute Sicherheit. Nehmen wir z. B. die Pässe, die nunmehr sicherheitstechnisch hochgerüstet sind mit elektronisch gespeicherten, biometrischen Gesichtserkennungs- und Fingerabdruckdaten. Die neuen Pässe wurden eingeführt, um den Identitätsmissbrauch zu verhindern, ein Phänomen, das es nach der frühen Einführung der fälschungssicheren Ausweise als Problemfeld nachweisbar nicht gab. In Wahrheit wird die Möglichkeit eines Identitätsdiebstahls aber erhöht, weil erst durch den neuen Pass biometrische Merkmale wie das Bild eines Passinhabers mit hoher Qualität weltweit verfügbar gemacht werden. Erst jüngst zeigte die Sendung „Panorama“ wie einfach es ist, in Mitgliedsstaaten der EU für Bürger aus anderen Ländern (Drittstaaten) EU-Pässe zu besorgen. Sie zeigte z. B. eine Agentur in St. Petersburg, deren Geschäftsfeld es ist, für Fremde Original-EU-Pässe zu beschaffen. Dafür haben wir jetzt Pässe, die – ist der Code erst mal geknackt - es ermöglichen, unsere Fingerabdrücke an jedem beliebigen Ort der Erde zu reproduzieren. Gerade im Ausland muss der Pass häufig auch aus der Hand gegeben werden, in vielen Hotels z. B. über Nacht, so dass die biometrischen Merkmale ausgelesen und für andere Zwecke verwendet werden können. Und welche Sicherheit ist gewonnen, wenn sich allein in Deutschland mehrere hunderttausend Personen illegal aufhalten? Nein, viele beschleicht der Verdacht, hier soll ein anderer Staat vorbereitet werden.

Ein weiteres erschreckendes Beispiel ist die Vorratsdatenspeicherung, ein System, das nicht einmal die sicherheitsfanatischen USA praktizieren. Die rechtliche Einschätzung der in 2007 eingeführten Regelungen zur Vorratsdatenspeicherung sind unter Ziff. 4.1 und 21.4 dieses Berichts zu finden. Vor der Abstimmung zur Vorratsdatenspeicherung im Bundestag habe ich mit einem Schreiben an die

Bremer Bundestagsabgeordneten versucht, diese dazu zu bewegen, dem Gesetz ihre Zustimmung zu verweigern. Meine wesentlichen Argumente sind auch in meiner Pressemitteilung vom 8. November 2007 enthalten, die Sie auf meiner Homepage finden (www.datenschutz-bremen.de/pressemitteilung.php?pressid=8595).

Das Unbegreifliche an der ganzen Entwicklung ist, dass alle Maßnahmen, von denen jetzt die Bevölkerung in Gänze getroffen wird, mit dem Argument „Terrorismusbekämpfung“ eingeführt, schon in naher Zukunft ganz anderen Zwecken dienen können. Das Rad, gespeicherte Daten für weitere neue Zwecke zu nutzen, wird immer ein Stück weiter gedreht. Schon jetzt wurde z. B. bei der Debatte um die Einführung der Vorratsdatenspeicherung deutlich, dass politische Kräfte sich dieser Daten gern bemächtigt hätten, um die Daten für die Verfolgung von Raubkopien der Musikindustrie zur Verfügung zu stellen. Das Gleiche erleben wir bei anderen jüngst geschaffenen technischen Infrastrukturen, die die Totalüberwachung eines Alltagsbereichs unserer Bürger zulassen. Auch mit der in Mautbrücken eingebauten Technik kann man mehr, nämlich die Beobachtung des gesamten Verkehrs auf den Bundesautobahnen, auch hier gibt es politische Bestrebungen, die Zweckbindung der Daten für die Abrechnung der Autobahngebühr aufzuweichen.

Zum Glück war bei vielen dieser Entwicklungen bisher das Bundesverfassungsgericht Bewahrer der Verfassung und leider nicht der Bundestag. Aber auch diese Entscheidungen können natürlich nicht das ganze Ausmaß der technischen Ausforschung des privaten Lebens durch öffentliche und staatliche Stellen mit den daraus resultierenden Folgen verhindern. Der Staat ist mittlerweile in der Informationsgesellschaft angekommen, aber er muss noch lernen, dass man mit dem Brotmesser nur Brot schneidet.

1.4 Kurangebot „Überwachungsfreie Ruheräume“

Aber auch einzelne Geschäftsbereiche der Wirtschaft rüsten auf. Mir gegenüber wird häufig Klage geführt über eine permanente „Bombardierung“ des Einzelnen durch technische Geräte, denen der Mensch sich immer mehr wehrlos ausgesetzt fühlt. So nimmt z. B. die Flut von Spam-Mails, unerwünschten SMS oder unnötigen Anrufen von Sprachcomputern laufend zu. Die gesellschaftlich erwartete oder vom Arbeitgeber verlangte ständige Erreichbarkeit wird zu nicht gewünschten wirtschaftlichen oder gelegentlich sogar kriminellen Aktivitäten von „Trittbrettfahrern“ mitgenutzt. Eine Vielzahl weiterer neuer Möglichkeiten tut sich durch in Handys integrierte Navigationssysteme und insbesondere die Funkchiptechnologie (RFID) auf. Alles in allem befürchte ich, nicht lange nach der Debatte über rauchfreie Zonen wird es eine Debatte über die Notwendigkeit zur Schaffung überwachungsfreier Räume geben.

1.5 Das Bankgeheimnis und die Metapher vom Schweizer Käse

Gesetzliche Regelungen, die den unmittelbaren elektronischen Zugriff auf Datensysteme der privaten Wirtschaft erlauben, nehmen zu. Eine Entwicklung, die übrigens zeigt, wie sinnvoll es ist, Datenschutzkontrolle – wie in Bremen von Anbeginn - in eine Hand zu geben. Auch bestärkt es mich in meiner seit Jahren geäußerten Auffassung, dass Regelungen für den rechtlich zulässigen Abgleich von Daten verschiedener verantwortlicher Stellen in einem „Black-Box-Verfahren“ eine Grundregelung im allgemeinen Datenschutzrecht haben sollten. Exemplarisch für diese eingangs genannte Entwicklung steht das Kontoabrufverfahren nach § 24 c Kreditwesengesetz (KWG) und §§ 93, 93 b Abgabenordnung (AO).

Die Zahl der Kontenabfragen öffentlicher Stellen stieg laut Presseberichten im Jahr 2007 bundesweit auf fast 100.000. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) stellte danach im vergangenen Jahr einen Anstieg um 15 Prozent im Vergleich zu 2006 fest. In insgesamt 93.560 Fällen sollen Behörden die Kontostammdaten abgefragt haben. Hinter dieser Zahl stehen insgesamt rund 200 Millionen Zugriffe auf Datenbanken der Kreditinstitute, denn jede Einzelabfrage nach passenden Kontoverbindungen löst eine virtuelle Suche in den Systemen aller rund 2.000 Banken hierzulande aus.

Eine Steigerungsrate ähnlich stark wie bei der Telefonüberwachung, die nicht mit einer Mehrung von Kontoeröffnungen erklärt werden kann. Sie kann vielmehr mit der Einführung einer voll elektronischen Abfrage zusammenhängen. Ich habe diesen Bereich erstmalig vor zwei Jahren untersucht und die Ergebnisse öffentlich gemacht (vgl. 28. JB, Ziff. 15.1). Das war noch die Einführungsphase. Eine Untersuchung der Rechtmäßigkeit vermehrter Abrufe kann in Bremen allerdings erst nach einer Wiederbesetzung des zuständigen Referats 50 in meinem Hause erfolgen.

In den thematischen Zusammenhang gehört auch der Beschluss des Bundesverfassungsgerichts zum Kontenabrufverfahren, mit dem die Karlsruher Richter unterstrichen haben, dass die angegriffenen gesetzlichen Bestimmungen die Abfrage von Kontostammdaten der Bankkunden und sonstiger Verfügungsberechtigter nicht "routinemäßig" oder gar "ins Blaue hinein" erlauben. Vor diesem Hintergrund sind die Planungen des Bundesministeriums für Finanzen kritisch zu betrachten, die zeigen, wo die Entwicklung hingeht. Die täglichen elektronischen Abrufmöglichkeiten sollen von jetzt 100 auf bis zu 5.000 Abrufe erweitert werden.

Darüber hinaus hat das Bundesverfassungsgericht den Gesetzgeber verpflichtet, den § 93 der Abgabenordnung nachzubessern, weil in der beanstandeten gesetzlichen Regelung der Kreis der zum Datenabruf berechtigten Behörden außerhalb der Finanzverwaltung nicht präzise festgelegt ist. Zukünftige Aufgabe wird es sein, gemeinsam mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) die Einhaltung der Vorgaben, etwa der Benachrichtigung sowie der Regelung, dass die Zugriffe lückenlos zu protokollieren sind, zu kontrollieren.

1.6 Besondere Regelungen zum Arbeitnehmerdatenschutz fehlen weiter

Die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die elektronische Überwachung von Beschäftigten am Arbeitsplatz oder z. B. die Erhebung des Gesundheitszustandes und psychologische Testverfahren bei der Einstellung, erfordern einen besonderen Schutz des Betroffenen durch bundeseinheitliche gesetzliche Regelungen. Dies fordern die Datenschutzbeauftragten des Bundes und der Länder seit Jahren, erneut in einer Entschließung im März 2007 (vgl. Ziff. 21.5 dieses Berichts).

1.7 Aus dem dunklen Keller kommt das Kabel fürs Internet

Den Stand der Verbreitung von Internetanschlüssen in deutschen Haushalten gibt die Übersicht „Indikatoren der Informationsgesellschaft“ unter Ziff. 24.4 dieses Berichts wieder. Sie zeigt, dass bereits mehr als die Hälfte der Deutschen sich mit den Problemen des Internets auseinandersetzen muss.

Früher begab man sich in den Wilden Westen, um Abenteuer zu erleben, heute kann man sich in ein Dschungel-Camp begeben, aber am interessantesten ist es immer noch im Internet. Die Risiken sind vielfältig, sie einzuschätzen, übersteigt die Vorstellungskraft und trotzdem, alle Welt tummelt sich dort, ob Otto-Normalverbraucher, Firmen oder Verwaltung, alle bewegen sich auf den unsicheren elektronischen Datenwegen. Ausgeklügelte Methoden beim Online-Banking leiten Überweisungen fehl, manche Menschen bedienen sich mit kriminellen Programmen gar selbst und buchen bei anderen mal rasch alles ab, was auf dem Konto ist, Viren-Attacken auf Computer, Spam-Mail, Mail-Angriffe, die Unternehmen für Tage lahm legen, heimliches Mitlesen oder das Ausspähen von Daten – um nur einige Erscheinungsformen zu nennen – schrecken die Nutzer zwar nicht ab, lassen sie aber oft nicht ruhig schlafen.

Einige Internet-Nutzer sind zu allem Überfluss dazu übergegangen gleich selbst ihre meist überschaubare kleine Idylle frei Haus in Bloggs, Bildern oder Videoclips zu liefern. Diese gelegentlich exhibitionistischen Darstellungen lassen mich aber keineswegs daran zweifeln, am Gedanken des Datenschutzes festzuhalten. Es ist nämlich etwas grundsätzlich Verschiedenes, ob sich jemand selbst in aller Öffentlichkeit auszieht oder ob dort jemand gegen seinen Willen entblößt wird.

Wir müssen uns nur von dem Gedanken verabschieden, dass das Internet ein sicheres Netz mit hohem Datenschutzstandard ist oder werden könnte. Dafür ist es überhaupt nicht konzipiert, es beginnt und endet eben oft in dunklen Kellern. Viele Surfer müssen feststellen, dass sie für all die bunten kostenlosen Internetangebote in Wahrheit oft mit ihren persönlichen Daten bezahlen müssen. Als Faustformel kann man empfehlen: „Mache nichts im Internet, was Du nicht auch vor allen Augen in der Öffentlichkeit tun würdest“.

Gleichwohl wollen viele Menschen sich nicht ungefragt mit einer Datenselbstbedienung Dritter abfinden. Eine aktive Netzgemeinde wehrt sich vielerorts gegen das allzu dreiste „Absaugen“ von Daten. Von Computer-Freaks herausgefundene und in Presseberichten publizierte Nachrichten wie „Weltherrschaft via Vista, Experten halten Microsofts neues Betriebssystem für indiskret“ bleiben nicht ohne Erfolg, das haben damals die Reaktionen auf den kleinen ET im Windows Mediaplayer „....nach Hause telefonieren“ gezeigt. Auch der Internetbranche wird bewusst, dass sie in punkto Datenschutz die Rechnung ohne den Wirt gemacht hat. Jedenfalls ist in den letzten Jahren festzustellen, dass sich führende Unternehmen mehr um Datenschutz und Datensicherheit in ihren Angeboten und Produkten kümmern und dies in ihren Erklärungen nachvollziehbar machen. Auch das Bundesministerium der Justiz durfte auf diesem Gebiet erste Erfahrungen sammeln (zum Urteil des BVerfG in diesem Zusammenhang vgl. Ziff. 4.4 dieses Berichts).

Anzumerken ist, dass ich natürlich eine Vielzahl von Bürgerbeschwerden erhalte, die sich auf Datenschutzverstöße im Internet beziehen. Nicht in allen Fällen kann ich tatsächlich helfen, weil mir zum einen eine hierfür ausreichende personelle Ausstattung fehlt, zum anderen oft der technische Aufklärungsaufwand in keinem Verhältnis zum ungewissen Erfolg steht.

1.8 Deine Internet-Suchmaschine kennt Dich

Derzeit steht bei den EU-Innenpolitikern die geplante Fusion zwischen Google und dem US-amerikanischen Online-Werbevermarkter DoubleClick auf dem Prüfstand. Beide Unternehmen gehören in ihren jeweiligen Geschäftsbereichen zu den Marktführern. DoubleClick ist einer der größten Anbieter auf dem Markt für Online-Banner-Werbung. Google ist bei den Suchmaschinen die Nummer Eins und Marktführer in Sachen kontextbezogener Webseiten- und Suchmaschinenwerbung. Nicht erst jetzt diskutieren die Datenschutzbeauftragten die Auswirkungen der umstrittenen Übernahme. Schon die bloße zunehmende Abhängigkeit von einer solchen Suchmaschine wie Google bei Wissenschaft, Politik und Verwaltung zwingen zu einer gesellschaftspolitischen Debatte. So liegt es auf der Hand, dass dann, wenn bestimmte Informationen gezielt auf die hinteren Seiten einer Suchmaschine verbannt werden oder gar ganz geblockt werden, wie z. B. für die VR China, dies Einfluss auf die Meinungsbildung hat. Die Abhängigkeit bei der Entscheidungsfindung von Suchmaschinen nimmt in allen gesellschaftlichen Bereichen zu. Eine gesellschaftliche Kontrolle dieser Suchmaschinen gibt es jedoch nicht.

Google macht mit seinem Werbesystemen Milliardenumsätze, die sich der börsennotierte Gigant natürlich nicht durch gesetzliche Vorgaben beschneiden lassen möchte. Wer "googeln" will, muss Werbung akzeptieren, so lautet Googles Grundsatz. Dabei werde lediglich die IP-Adresse gespeichert.

Eine Datenpanne, die dem Mitbewerber AOL Anfang August 2006 unterlief, spricht eine andere Sprache. Die Suchverläufe von mehr als einer halben Million AOL-Nutzern wurden damals versehentlich online gestellt. IP-Adressen wurden nicht genannt, dafür alle Suchanfragen mit Datum und Uhrzeit sowie die angeklickten Webseiten. Insidermeldungen zu Folge stammten dabei die Daten nicht von AOL, sondern von Google, weil AOL keine eigene Suchmaschine einsetze, sondern über Google für sich suchen lässt. Fazit war, dass mittels der veröffentlichten Daten aus den Suchläufen es mit einfachen technischen Mitteln gelang, einzelne AOL-Kunden mit Namen und Anschrift zu identifizieren. Damit waren bereits ohne IP-Adresse Rückschlüsse auf das Surfverhalten und die Interessen konkreter Nutzer möglich. Der Öffentlichkeit wurde zum ersten Mal deutlich, dass alles aufgezeichnet wird, was die Benutzer tun. Google gelingt das, indem jedem Surfer beim erstmaligen Besuch der Google-Webseite eine eindeutige Identifikationsnummer zugewiesen wird, die in einer kleinen Textdatei, einem Cookie, auf seiner Festplatte gespeichert wird. Die Daten, die unter dieser Nummer eifrig gesammelt werden, dienen dazu, Profile anzulegen, um die Nutzer mit gezielter Werbung einzudecken.

Mit der Fusion von Google und DoubleClick verbinden sich die beiden größten globalen Datenbanken mit Daten von Konsumenten. Hinzu tritt, dass Google auch noch andere personenbeziehbare Internet-Dienstleistungen anbietet, wie Google Mail, Google Talk oder Google Kalender (näheres vgl. Ziff. 4.2 dieses Berichts). Ein Google-Slogan lautet: “Kein Aufwand, keine Kosten: Einfache und leistungsstarke Tools zur Kommunikation und Zusammenarbeit für Organisationen und Schulen“. Aber hat das börsenorientierte Unternehmen tatsächlich etwas zu verschenken?

Darüber hinaus hat Google Presseberichten zufolge im April 2007 einen Patentantrag für eine Methode eingereicht, mit der sich die psychologischen Profile von Millionen Menschen erzeugen lassen, indem ihre Aktivitäten bei Online-Spielen heimlich verfolgt werden. Aus dem Online-Verhalten

ließen sich Aufschlüsse über Persönlichkeit und Vorlieben der Spieler ziehen, um diese Profile an Interessenten zu verkaufen, die in Spielen werben wollen.

Das Patent wurde nach dem Bericht der britischen Zeitung Guardian in den USA und in Europa eingereicht. Der Newsticker von www.heise.de meldete am 12. Mai 2007: Der Patentbeschreibung zufolge eigneten sich Rollenspiele wie „World of Warcraft“ oder „Second Life“ am besten für die Erzeugung psychologischer Profile, da hier die Spieler mit anderen interagieren und Entscheidungen treffen, die denen ähnlich sein könnten, die sie im wirklichen Leben treffen. Aus den Dialogen könne man herauslesen, ob ein Benutzer beispielsweise vorsichtig, höflich, aggressiv, verletzend oder ruhig sei, zudem ließen sich aus dem Spielverhalten auch Persönlichkeitseigenschaften wie kooperatives, aggressives, riskantes Verhalten schließen. Damit könne man Werbung gezielter schalten, so der Patentantrag. Wer beispielsweise viel Zeit auf Erkundungen verwendet, könnte Interesse an Urlaubsangeboten zeigen, wer viel mit anderen Spielern spricht, wäre vielleicht der Handy-Werbung gegenüber empfänglich. Wer länger als zwei Stunden am Stück spielt, könne auf Werbung für Pizzas, Kaffee oder Getränke ansprechen.

Beobachtet würden nicht nur Online-Spiele, sondern auch Spiele auf Konsolen mit einer Internet-Verbindung. Auch aus gespeicherten Spielinformationen ließen sich Informationen gewinnen. Eine Personenbeziehbarkeit ist auch hier nicht ausgeschlossen. Damit werden z. B. auch künftige Arbeitgeber an diesen Psychogrammen der überwiegend jugendlichen Spieler interessiert sein. Da bleibt es ein schwacher Trost, dass nach Auskunft von Google das Unternehmen keine baldige Anwendung der beschriebenen Technik beabsichtige. Es soll sich dabei nur um einen von vielen Patentanträgen handeln, die Google gestellt habe.

Aber damit nicht genug, letzten Meldungen zufolge will Google in das Mobilfunkgeschäft einsteigen. Entwickelt wird ein Handy-Betriebssystem namens Android, das in Zusammenarbeit mit über 30 Technologie- und Telekomkonzernen entwickelt werden soll, teilte das Unternehmen mit. Die Handydaten gekoppelt mit Google-Earth und Google weiß, wo Sie sind und was Sie dort wahrscheinlich suchen.

Wir, die Datenschutzbeauftragten in der EU sind daher gut beraten, wenn wir weiterhin die Entwicklung im Auge behalten. Ich habe auf dieses Thema erneut öffentlich hingewiesen (vgl. BN/WK vom 20 Juni 2007, „Datenschützer kritisieren Google: Suchmaschine speichert Recherchen 18 Monate/Benutzerverhalten wird transparent“). Die Auseinandersetzung mit Google um die Speicherfristen (vgl. Ziff. 4.2 dieses Berichts) kann daher nur ein erster Schritt gewesen sein.

1.9 Kinderschutz

Die Wogen in der öffentlichen Meinung schlagen zu recht hoch, wenn Kindesvernachlässigungen bis hin zum Tod der Kinder als Folge bekannt werden. Seit dem Fall „Kevin“ in Bremen hat es eine ganze Reihe ähnlich gelagerter Fälle in anderen Bundesländern gegeben, die mich alle nur fassungslos machen, wie Eltern es fertig bringen, so mit hilflos ihnen ausgelieferten Geschöpfen umzugehen. Die Politik erfährt daher von mir jegliche Unterstützung, wenn es darum geht, Wege zu finden, diese Gräueltaten zu verhindern. Allerdings muss auch gesagt werden, dass alle bisher öffentlich bekannt gewordenen Fälle nicht deshalb geschehen konnten, weil es den zuständigen Stellen an Informationen fehlte. Ich bin daher nicht bereit, daran mitzuwirken, ein ausuferndes Überwachungsinstrument (womöglich basierend auf heimlichen Hinweisen, Verdächtigungen oder gar Verleumdungen) gegenüber allen Eltern aufzubauen, sondern es muss darum gehen, gezielt Problemgruppen in eine konkrete Begleitung zu nehmen, wobei hier zum Beispiel Drogenabhängigkeit, Alkoholismus und psychische Erkrankungen Indiz sein können. Aber auch hier ist es meine Aufgabe, darauf zu achten, dass deren Grundrecht auf informationelle Selbstbestimmung gewahrt wird.

Am 19. Dezember 2007 hat die Ministerpräsidentenkonferenz in Berlin getagt und sich intensiv mit den Problemen der Kindesvernachlässigung und -misshandlung beschäftigt. Dabei hat die Bundesregierung erklärt, zusammen mit den Ländern zu prüfen, welche Änderungen erforderlich sind, um einen reibungslosen Informationsaustausch zum Schutz gefährdeter Kinder in überforderten Familien zu gewährleisten. Ich bin bereit, die Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales bei diesem Prozess zu begleiten, um festzustellen, ob und gegebenenfalls welcher gesetzgeberische Handlungsbedarf für den Aufbau eines angemessenen Informationsaustausches (Frühwarnsystem) erforderlich ist. Dabei muss aber im Auge behalten werden, dass alle Stellen, die ein Behandlungs- oder Hilfeangebot an diesen kritischen Kreis von Eltern und deren Kinder machen, bei Schaffung einer gesetzlichen Übermittlungspflicht wohlmöglich gerade von Eltern dieser Klientel nicht mehr aufgesucht werden, um die Leiden der Kinder zu vertuschen, was das Elend der betroffenen Kinder noch vergrößern dürfte. Ich bin daher der Meinung, dass alles, was über den gesetzlichen Status quo hinaus geregelt werden soll, abgewogen und mit den beteiligten Berufsgruppen diskutiert werden muss.

Unter Zugrundelegung der vorgenannten Prämissen habe ich die verschiedenen Projekte des Ressorts auf diesem Gebiet begleitet, im Einzelnen vgl. unter Ziff. 12.3 dieses Berichts.

1.10 Der 30. Bericht

Die Zahl 30 dieses Datenschutzberichtes ist nicht gleichbedeutend mit „30 Jahre Datenschutz im Lande Bremen“, denn dieser Termin liegt erst im Sommer 2008. Der erste Datenschutzbericht für das Land Bremen musste nämlich bereits nach einem halben Jahr geschrieben werden. Zum 25-jährigen Bestehen des Datenschutzes in Bremen hatte ich noch eine CD herausgebracht mit vielen Artikeln und multimedialen Darstellungen. Einen Teil davon konnte ich später auf meine Homepage übertragen, zu finden unter: www.datenschutz-bremen.de/ds25.php. Ob es mir im Sommer 2008 gelingen wird, auch nur in irgendeiner Form dieses Jubiläum zu begehen, erscheint äußerst fraglich angesichts der angespannten personellen und finanziellen Situation meiner Dienststelle (vgl. Ziff. 20.4 dieses Berichts). Ideen gäbe es genug und vielleicht kommt bis dahin noch ausreichende Unterstützung.

1.11 19.000 Zugriffe pro Monat

Das ist kein Druckfehler: Die Internetseiten des LfDI Bremen wurden 2007 monatlich im Durchschnitt 19.000-mal besucht, das erbrachte die Statistik des Providers. Da war selbst ich sehr überrascht. Im Jahr also über 200.000 Besuche. Ich werte dies als ein Zeichen dafür, dass der Datenschutz bei den Bürgern Hochkonjunktur hat. Die Statistik zeigt darüber hinaus auch, dass eine wesentliche Entlastung der Arbeit mit dem Angebot auf der Homepage verbunden ist.

1.12 Datenpannen

Sei es, dass die Steuerdaten von über 20 Millionen Briten durch eine Datenpanne verloren gingen, sei es, dass der amerikanische Geheimdienst NSA die Telefonverbindungsdaten von 200 Millionen Amerikanern rechtswidrig gesammelt hat oder sei es, dass ein Offizier der Royal Navy sein Notebook mit Informationen über 600.000 Bewerber und Angehörige der Marine verloren hat, es sind nicht die Skandale, die zu mehr Datenschutz führen. Hierfür braucht man einen langen Atem und ein sich kontinuierlich entwickelndes, die technischen Gefahren mit einbeziehendes System von Verantwortung, verbunden mit einem organisierten Risikomanagement. Ich versuche, diesen Prozess seit Jahren in der Bremer Verwaltung fest zu verankern. Die genannten Datenskandale machen m. E. nur deutlich, welche Datenmengen sich mittlerweile in staatlichem Besitz befinden.

2. Betriebliche und behördliche Beauftragte für den Datenschutz

2.1 Workshops der behördlichen Beauftragten für den Datenschutz

Um die behördlichen Datenschutzbeauftragten bei der Wahrnehmung ihrer Aufgaben zu unterstützen, habe ich im Frühjahr und Herbst des Berichtsjahres jeweils an einem Nachmittag weitere Workshops durchgeführt. Schwerpunktthema der Veranstaltung im Frühjahr war die Präsentation einer von mir erstellten „Orientierungshilfe zur Entwicklung eines Entsorgungskonzepts zur Datenträgervernichtung“. Die Entsorgung von Datenträgern als letzte Phase der Datenverarbeitung ist ein Vorgang, für den angemessene datenschutzrechtliche Regelungen zu treffen sind. Ich habe die Teilnehmer des Workshops darauf hingewiesen, welche Fragen hinsichtlich der Entsorgung zu klären sind und wie sie gelöst werden können. Ich habe einige Anregungen aus der Runde noch in mein Konzept eingearbeitet und dies dann in einer Orientierungshilfe veröffentlicht, die über mein Internetangebot abgerufen werden kann (http://www.datenschutz-bremen.de/pdf/datenloeschung.pdf).

Der im Herbst des Jahres durchgeführte Workshop befasste sich schwerpunktmäßig mit dem Thema „Informationsfreiheit und Datenschutz“. Der Anspruch auf Zugang zu amtlichen Informationen ist abzuwägen mit dem Recht Betroffener auf informationelle Selbstbestimmung. Das Interesse an der Gewährung des Zugangs zu öffentlichen Informationen steht dabei im Konflikt mit den schutzwürdigen Interessen Dritter, wobei ein gerechter Interessenausgleich gefunden werden muss. In den Workshops gab es mit den Teilnehmern rege Diskussionen.

Die Workshopteilnehmer erhielten in den Workshops außerdem wieder die Möglichkeit, bei der Wahrnehmung ihrer Tätigkeit gesammelte Erfahrungen auszutauschen, wovon sie intensiv Gebrauch machten. Einige Teilnehmer schilderten hierbei Probleme, die in ihren Dienststellen im Hinblick auf die Akzeptanz und das Verständnis ihres Amtes bestehen. Die uneingeschränkte Wahrnehmung der den behördlichen Datenschutzbeauftragten nach dem Bremischen Datenschutzgesetz zugewiesenen gesetzlichen Aufgaben muss von der Dienststellenleitung sichergestellt sein. Dabei ist es nicht Aufgabe der behördlichen Datenschutzbeauftragten, die von den Dienststellen zu erstellenden Datenschutzkonzepte oder Verfahrensbeschreibungen selbst zu fertigen. Im Hinblick auf eine den gesetzlichen Anforderungen entsprechende Datenverarbeitung ist es den Dienststellen nicht gestattet, Aufgaben, die nicht zum gesetzlich vorgesehenen Aufgabenkreis der behördlichen Datenschutzbeauftragten gehören, ihnen zu übertragen. Nach § 7 a Abs. 4 BremDSG wirkt der behördliche Datenschutzbeauftragte auf die Einhaltung des Bremischen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz hin. Insbesondere hat er z. B. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen. Die Kontrollfunktion ergibt sich darüber hinaus auch aus § 7 Abs. 2 BremDSG, wonach der behördliche Datenschutzbeauftragte bei der Einführung oder Änderung automatisierter Verfahren, mit denen personenbezogene Daten verarbeitet werden, eine Vorabkontrolle durchzuführen hat. Ich beabsichtige, die einzelnen Dienststellen auf die Rechtslage noch einmal gesondert aufmerksam zu machen.

Wegen des starken Interesses an meinen Workshops – teilweise musste ich wegen großer Teilnehmerzahlen bis zu drei Veranstaltungen durchführen - ist geplant, auch im Jahr 2008 mit den behördlichen Datenschutzbeauftragten Workshops zu aktuellen ressortübergreifenden Themen durchzuführen. Darüber hinaus versuche ich, den Datenschutzbeauftragten Unterstützung für die Wahrnehmung ihrer Tätigkeit durch mein Internetangebot zu geben.

2.2 Auslegung der neuen Regelungen zur Bestellung betrieblicher Beauftragter für den Datenschutz

Durch das „Erste Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft“ vom 22. August 2006 (BGBl. 2006, 1970) wurden verschiedene Vorschriften des Bundesdatenschutzgesetzes (BDSG) geändert. Die neuen Regelungen enthalten Klarstellungen, allerdings auch unbestimmte Rechtsbegriffe, die auslegungsbedürftig sind.

Für die Sitzung der Konferenz der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich im Herbst 2006 in Bremen, erstellte ich eine Vorlage, um eine Abstimmung unter den Aufsichtsbehörden über die Auslegung der neuen Regelungen herbeizuführen. Die anschließende Diskussion und verschiedene Stellungnahmen führten zu einer Annäherung der verschiedenen Standpunkte. Jedoch konnte in wenigen Punkten keine Einigkeit erzielt werden. Ich werde meine Auslegungs- und Anwendungshilfe als Merkblatt für Datenverarbeiter für den nicht öffentlichen Bereich im Land Bremen auf meiner Homepage veröffentlichen, um den betroffenen Stellen eine praktische Hilfestellung zu geben.

3. Bremisches Datenschutzaudit u. a.

3.1 Bremisches Datenschutzaudit – Zulassung eines Auditors

Im Berichtsjahr habe ich zum zweiten Mal seit Inkrafttreten der Bremischen Datenschutzauditverordnung (BremDSAuditV) einen Auditor zugelassen. Das zertifizierte Verfahren VERA unterstützt die Verwaltung arbeitsmarktpolitischer Mittel des Landes Bremen. Es umfasst u. a. die Verarbeitung personenbezogener Daten von Teilnehmern an Arbeitsförderungsmaßnahmen insbesondere der Verwaltung und die Vermittlung von Integrationsjobs („Ein-Euro-Jobs“) in der Stadt Bremen durch die Bremer Arbeit GmbH (BAG).

Die BAG hatte mir einen Gutachter zur Zulassung als Auditor für das Verfahren VERA vorgeschlagen. Nach Prüfung des Vorliegens der Voraussetzungen für die Wahrnehmung der Tätigkeit (fachliche Eignung, persönliche Zuverlässigkeit und Unabhängigkeit) habe ich den Gutachter zugelassen. Der erfolgreiche Abschluss der Verfahrensprüfung durch den Auditor berechtigt die BAG, für einen Zeitraum von zwei Jahren das bremische Datenschutzgütesiegel für das auditierte Verfahren zu verwenden.

3.2 Bundesdatenschutzauditgesetz – zum Entwurf des BMI

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat den Datenschutzbeauftragten der Länder einen Entwurf zum Bundesdatenschutzauditgesetz (BDSAuditG) aus dem Bundesministerium des Innern (BMI) zur Verfügung gestellt mit Bitte um Einschätzung, um sie in seiner Stellungnahme gegenüber der Bundesregierung zu berücksichtigen. Ich habe dazu eine Stellungnahme abgegeben, zum einen, weil Bremen neben Schleswig-Holstein des einzige Land mit praktischen Erfahrungen auf dem Gebiet ist, zum anderen, weil nach dem Entwurf auf mich als Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich neue Aufgaben zukämen. Einige will ich kurz skizzieren.

Im Gegensatz zur Regelung in Bremen ermöglicht § 9 a Satz 1 BSDG und demzufolge § 1 Abs. 1 BDSAuditG-E neben datenverarbeitenden bzw. verantwortlichen Stellen auch Anbietern von Datenverarbeitungssystemen und –programmen ein Audit für Datenschutzkonzepte und ihre technischen Einrichtungen. Verkürzt kann man auch von einem Verfahrens- und Produktaudit sprechen. Die bremische Auditregelung hat auf ein Produktaudit verzichtet, weil Produkte nur in ihrer technischen Umgebung und ihrem konkreten Einsatzbereich sinnvoll beurteilt werden können.

Dies wird an folgendem Beispiel deutlich: Eine Gesprächsaufschaltvorrichtung ist eine Einrichtung, mit der sich ein Dritter in einer Telefonanlage bemerkt oder unbemerkt in ein laufendes Telefonat hörend oder auch sprechend einschalten kann. Selbst wenn eine Telefonanlage die technische Möglichkeit der Unterdrückung zur Gesprächsaufschaltung enthielte, macht es aus meiner Sicht keinen Sinn, die technischen Funktionen einer Telefonanlage abstrakt zu betrachten, sondern nur konkret in ihrer Einsatzumgebung mit den tatsächlich eingestellten differenzierten Möglichkeiten.

Ich habe daher den BfDI gebeten, noch einmal darüber nachzudenken, ob die Produktauditierung in der vorgesehenen Form in die gesetzliche Regelung des Bundes mit aufgenommen werden soll.

Leitfaden meiner Stellungnahme waren die bremischen Regelungen. Diese sehen vor, dass das Datenschutzkonzept und die tatsächlich getroffenen technischen Einrichtungen einer Datenverarbeitungsanlage wesentlicher Bestandteil der Bewertung und Prüfung sind. Die bremischen Regelungen sehen darüber hinaus nur eine konkrete Bestellung von Sachverständigen für einzelne Verfahren vor. Es gibt nach meiner Einschätzung keine Sachverständigen, die eine Allround-Eignung haben für jedwedes technische Verfahren. Um Datenschutzrisiken feststellen zu können, muss ein Sachverständiger die grundsätzliche Wirkweise der zu begutachtenden technischen Verfahren beherrschen. Dies lässt sich jeweils nur konkret und nicht vorab abstrakt für alle Verfahren feststellen. Ich habe daher Bedenken geltend gemacht, wenn Sachverständige in einem allgemeinen Verfahren unabhängig von einem konkreten Auditierungsverfahrens bestellt werden würden.

4. Internet, Telekommunikation, Teledienste

4.1 Vorratsdatenspeicherung ist nun Gesetz

Ich habe zusammen mit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt verfassungsrechtliche Bedenken gegen das Gesetzgebungsverfahren zur Einführung der Vorratsdatenspeicherung geäußert. Die Bürger müssen sich weiterhin frei und unbeobachtet in ihrer Kommunikation fühlen können! Die gesetzlichen Regelungen stellen einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht aller Bundesbürger dar. Betroffen sind unterschiedslos auch Journalisten, Heilberufler wie Ärzte und Psychiater, Rechtsanwälte, Sozialarbeiter und Seelsorger.

Mit dem Gesetz entstehen Datensammlungen ungeheueren Ausmaßes. Es werden zunehmend präventive Instrumente mit großer Streubreite für die Terrorabwehr eingesetzt, die sich im Vorfeld einer konkreten Gefahr oder gar nur eines Gefahrenverdachts bewegen. Damit werden harmlose Verhaltensweisen völlig Unbeteiligter staatlichen Maßnahmen ausgesetzt. Die Speicherung von Daten auf Vorrat ist aus Sicht des Datenschutzes nicht erforderlich und stets unverhältnismäßig.

Die vielen Proteste gegen die Vorratsdatenspeicherung zeigen im Übrigen, dass diese Maßnahmen von weiten Teilen der Bevölkerung abgelehnt werden.

Der Bundestag hat in der vergangenen Legislaturperiode eine bundesdeutsche Regelung zur Vorratsdatenspeicherung mehrheitlich noch abgelehnt. Auch der wissenschaftliche Dienst des Bundestages hat in einer gutachterlichen Stellungnahme erhebliche verfassungsrechtliche Bedenken angemeldet. Irland hat eine Nichtigkeitsklage beim Europäischen Gerichtshof eingereicht. Vom EuGH wird in Kürze eine Entscheidung dazu erwartet.

Ich hatte daher in einem Brief an die Bremer Bundestagsabgeordneten appelliert, sich nicht zu einer Entscheidung drängen zu lassen (vgl. dazu auch www.datenschutz-bremen.de/pressemitteilung.php?pressid=8595), da EU-rechtliche und verfassungsrechtliche Fragen noch nicht abschließend geklärt seien. Ich bat die Abgeordneten, der Gesetzesvorlage nicht zuzustimmen, wenigstens aber die Entscheidung des EuGH abzuwarten.

Trotz der vorgetragenen datenschutzrechtlichen Bedenken hat der Bundestag am 9. November 2007 die Regelungen zur Vorratsdatenspeicherung verabschiedet (BR-Drs. 275/07). Sie werden überwiegend am 1. Januar 2008 in Kraft treten. Das Bundesgesetz verpflichtet die Anbieter von Telekommunikations- und Internetdiensten, umfangreiche Verkehrsdaten der Telefon- und Internetnutzung (zum Beispiel Rufnummern oder sonstige Kennungen des anrufenden oder angerufenen Anschlusses, elektronisches Postfach, IP-Adressen, Beginn und Ende der Verbindung, Standorte wie genaue Bezeichnung der genutzten Funkzellen) für ein halbes Jahr auf Vorrat zu speichern. Hiermit will die Bundesregierung die europäische Richtlinie zur Vorratsspeicherung umsetzen, welcher sie zugestimmt hat.

Kaum ist das Gesetz verabschiedet, zeichnet sich jetzt schon ab, was viele Kritiker vorausgesagt haben. Die Datenbestände wecken Begehrlichkeiten. Obwohl die Neuregelungen noch nicht einmal wirksam sind, fordert der Rechtsausschuss des Bundesrates in einer aktuellen Empfehlung eine gravierende Nachbesserung. Die Daten sollen nicht nur hoheitlichen Zwecken wie der Gefahrenabwehr oder der Strafverfolgung dienen, sondern auch zur Durchsetzung der Ansprüche von Urheberrechtsinhabern. Eine derartige Regelung würde eine weitere Schwächung des Rechts auf informationelle Selbstbestimmung der Bürger bedeuten. Exemplarisch für viele Betroffene haben

bereits jetzt Vertreter verschiedener Berufsgruppen gegen das Gesetz Verfassungsbeschwerde eingelegt.

4.2 „Datenkraken“ im Internet

Rund 90 Prozent der deutschen Internetnutzer verwenden die Suchmaschine Google, um Informationen aus dem Internet zu erhalten. Ich gehe davon aus, dass sich die Bremer Internetnutzerinnen und –nutzer dieser Suchmethode in gleichem Maße bedienen. Für die schnellen und komfortablen Recherchemöglichkeiten ist aus datenschutzrechtlicher Sicht allerdings ein hoher Preis zu zahlen. Suchmaschinen bergen eine erhebliche Gefährdung für die Privatsphäre der Nutzer. Es lassen sich detaillierte Profile von Interessen, Ansichten und Aktivitäten über verschiedenste Bereiche erstellen (z. B. Berufsleben, Freizeit, aber auch über besonders sensible Daten wie politische Ansichten oder sexuelle Präferenzen). Die Suchanfragen sind alles andere als anonym. Viele Suchmaschinen speichern bei Suchanfragen den Eingabetext und die Uhrzeit sowie die IP-Adresse. Es besteht die Möglichkeit, Nutzer zu identifizieren. Diese Gefahr besteht insbesondere dann, wenn zusätzliche Informationen aus zugehörigen Angeboten verwendet werden (E-Mails, Bloggs, etc.)

Besonders brisant sind auch die selbstgesetzten Speicherfristen der Suchmaschinenanbieter für Suchanfragen. Die großen Anbieter von Suchmaschinen speichern die Anfragen zwischen 13 und 18 Monate. Diese Speicherfristen sind nicht datenschutzkonform. Schon im November 2006 hat die 28. Internationale Konferenz der Datenschutzbeauftragten in London eine Entschließung zum Datenschutz bei Suchmaschinen gefasst. Darin werden Anbieter von Suchmaschinen aufgefordert, künftig keine personenbezogenen Daten (wie IP-Adressen) nach dem Ende der Nutzung zu speichern. Auf diese Weise soll verhindert werden, dass personenbezogene Daten der Nutzer dem Zugriff Dritter ausgesetzt sind. Hintergrund ist die Veröffentlichung von beinahe 20 Millionen scheinbar anonymisierten Suchanfragen durch AOL in den USA im Sommer 2006.

Ein weiteres Problem ist der sog. Cache (Zwischenspeicher) bei Suchmaschinen. Inhalte von Internetseiten, die längst nicht mehr online sind oder inhaltlich überarbeitet wurden, sind bei Suchmaschinen wie Google im Cache noch immer vorhanden und abrufbar. Die Möglichkeit auf nicht mehr aktuelle Inhalte zuzugreifen, kann zu erheblichen Problemen führen. So können Informationen veraltet oder falsch sein oder die Betroffenen möchten nicht mehr, dass sie einer breiten Öffentlichkeit zur Verfügung stehen. Nach dem deutschen Datenschutzrecht hat zwar jeder Betroffene das Recht, Daten berichtigen und löschen zu lassen. Schwierig ist aber die Durchsetzbarkeit dieser Rechte, wenn sich der Suchmaschinenbetreiber in den USA befindet. Man sollte sich daher stets vor Veröffentlichung von Inhalten im Internet der langfristigen Verfügbarkeit bewusst sein (vgl. 29. JB, Ziff. 4.3).

4.3 Veröffentlichung personenbezogener Daten im Internet

Wie auch in den letzten Jahren erhielt ich im Berichtsjahr wieder viele Beschwerden bezüglich Veröffentlichungen personenbezogener Daten im Internet. Es wurden Namen veröffentlicht und diese oft mit weiteren Daten wie Adresse, Krankheiten oder Berufsbezeichnung verknüpft. In der Veröffentlichung von personenbezogenen Daten im Internet kann ein erheblicher Eingriff in das Recht auf informationelle Selbstbestimmung liegen, welcher bußgeldwert ist. Grundsätzlich ist die Veröffentlichung personenbezogener Daten nur mit der Einwilligung der Betroffenen zulässig. Auch im Rahmen einer Interessenabwägung sind die schutzwürdigen Belange der Betroffenen an dem Ausschluss der Veröffentlichung ihrer Daten regelmäßig höher zu bewerten als das Interesse der verantwortlichen Person an der Veröffentlichung.

Ein weiteres Problem der Veröffentlichung im Internet ist die einfache Recherchierbarkeit. Da wundern sich des Öfteren Bewerber, warum sie von potentiellen Arbeitgebern trotz guter Qualifikation abgelehnt wurden. Die Begründung hierfür kann eine Internetveröffentlichung sein. Auch Personalchefs nutzen Suchmaschinen. Stoßen sie auf freizügige Fotos oder beleidigende Äußerungen der Bewerber, kann dieses der Grund für die Absage sein. Aus diesem Grund appelliere ich auch an alle Internetnutzer, sich genau zu überlegen, was man tatsächlich im Internet von sich preisgeben möchte. Da zudem die Gefahr von Verwechslungen besteht, empfehle ich Bewerbern zu überprüfen, ob zu namensgleichen Personen Veröffentlichungen existieren, mit denen man nicht in Zusammenhang gebracht werden möchte. In diesen Fällen sollte man potentielle Arbeitgeber darauf hinweisen, dass keine Identität besteht.

4.4 Unzulässige Registrierung von Website-Besuchern

Das Amtsgericht Berlin Mitte hat mit Urteil vom 27. März 2007 dem Bundesministerium der Justiz (BMJ) untersagt, personenbezogene Daten, die im Zusammenhang mit der Nutzung von dessen Internetportal übertragen werden, über das Ende des Nutzungsvorgangs hinaus zu speichern. Die Aufbewahrung solcher Kommunikationsspuren ermögliche es, das Surf- und Suchverhalten von Internetnutzern detailliert nachzuvollziehen. In einer solchen Vorratsprotokollierung liege eine Verletzung des Rechts auf informationelle Selbstbestimmung. Insbesondere dürften IP-Adressen nicht archiviert werden, weil es durch die Zusammenführung der personenbezogenen Daten mit Hilfe Dritter bereits jetzt ohne großen Aufwand in den meisten Fällen möglich sei, Internetnutzer aufgrund ihrer IP-Adresse zu identifizieren.

Das Landgericht Berlin hat die Entscheidung des Amtsgerichts im Wesentlichen bestätigt und nur insoweit modifiziert, als dass Namen der abgerufenen Datei bzw. Seite, Datum und Uhrzeit des Abrufs, die übertragene Datenmenge sowie die Meldung, ob der Abruf erfolgreich war, gespeichert werden dürfen, wenn die IP-Adresse nicht gespeichert wird. Da es sich bei diesen Angaben um keine personenbezogenen Daten handelt, liegt in der Modifizierung keine Verschlechterung für die Rechte der Betroffenen.

Das BMJ erstellt inzwischen nur noch anonyme Statistiken über die Nutzung seines Internetportals. Auf die Aufzeichnung von IP-Adressen wird fortan verzichtet. Ich berichte über das Urteil, weil die grundlegenden Ausführungen sowohl von öffentlichen wie von privaten Stellen beim Betreiben von Internetportalen zu beachten sind.

4.5 Elektronische Post und Datenschutz

E-Mail ist mittlerweile ein sehr stark eingesetztes Kommunikationsmittel und aus dem täglichen Leben nicht mehr wegzudenken, weder beruflich noch privat. Die datenschutzrechtlichen Vorgaben, die beim Einsatz von E-Mail-Systemen gerade vom Arbeitgeber zu beachten sind, sind vielfältig.

Ich habe unter http://www.datenschutz-bremen.de/technik/e_post.php auf meiner Internet-Seite eine Orientierungshilfe zum Umgang mit elektronischer Post veröffentlicht, in der auch auf die Gefahren hingewiesen wird, die der E-Mail-Einsatz mit sich bringt.

4.6 E-Government

Ausgehend von den Erfahrungen mit BundOnline 2005 und Deutschland-Online hat die Bundesregierung am 13. September 2006 das Programm E-Government 2.0 beschlossen und die Bundesressorts beauftragt, sich aktiv zu beteiligen . Die einzelnen Projekte und Ziele sind unter www.verwaltung-innovativ.de zu finden. Bis zum Jahr 2010 sollen „gewünschte Online-Dienste des Staates im erforderlichen Umfang elektronisch genutzt werden können“. Dazu soll auch ein elektronischer Personalausweis eingeführt werden, mit dem sich die Bürger im Netz ausweisen können. Mehr Sicherheit im Internet für die Bürgerinnen und Bürger sowie eine bessere Steuerung beim Einsatz von Informations- und Kommunikationstechnologien in der öffentlichen Verwaltung sind die Schwerpunkte der diesjährigen Themen bei der Weiterentwicklung von E-Government-Anwendungen zwischen Bund, Ländern und Kommunen. Eine weitere Koordinierung der Rahmenbedingungen des staatlichen Einsatzes moderner Informations- und Kommunikationstechnologien steht dabei ebenso im Vordergrund. Auch die Umsetzung der EU-Dienstleistungsrichtlinie bedarf der Begleitung durch den Datenschutz. Bremen nimmt auf dem Feld der „elektronischen Verwaltung“ ohnehin seit Jahren eine Vorreiterrolle wahr, ich verstehe mich dazu, die ehrgeizigen Ziele mit gutem Rat zum Datenschutz in den Projekten zu begleiten.

5. Medien

5.1 Das neue Telemediengesetz

Am 1. März 2007 ist das neue Telemediengesetz (TMG) in Kraft getreten. Dieses soll mit dem Rundfunkstaatsvertrag das bisherige Teledienstegesetz, Teledienstedatenschutzgesetz (TDDSG) sowie den Mediendienste-Staatsvertrag ersetzen. Die Zusammenfassung der wirtschaftsbezogenen Regelungen in einem bundeseinheitlichen (Telemedien)Gesetz soll ermöglichen, die Rechtslage besser an die Konvergenz der neuen Medien anzupassen. Zudem wurde durch die Einführung des TMG gleichzeitig die EG-Richtlinie 2000/31/EG über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft in nationales Recht umgesetzt.

Im Einzelnen lassen sich folgende Änderungen festhalten: Die Trennung zwischen Telediensten und Mediendiensten wird aufgegeben. Es gibt zukünftig nur noch Telemedien. Vom TMG erfasst werden alle Informations- und Kommunikationsdienste, die nicht ausschließlich dem Telekommunikations- oder Rundfunkbereich zuzuordnen sind. Dabei kann es sich etwa um Online-Angebote von Waren und Dienstleistungen mit sofortiger Bestellmöglichkeit, zeitversetztes Video on Demand, Weblogs, Online-Dienste wie Internet-Suchmaschinen oder Internet-Foren oder die kommerzielle Verbreitung von Informationen über Waren und Dienstleistungen per E-Mail handeln.

Bezüglich der Regelungen zur Haftung und Störereigenschaft haben sich keine Veränderungen ergeben. Das TMG schränkt aber den Adressatenkreis in Hinblick auf die Informationspflichten ein. Hiernach haben nur Diensteanbieter für geschäftsmäßige Telemedien, Informationen wie z. B. Namen oder Angaben für eine schnelle Kontaktaufnahme leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten. Geschäftsmäßige Angebote liegen nur dann vor, wenn diese in der Regel gegen Entgelt angeboten werden. Weiterhin stuft das TMG Spam-Mails nunmehr als Ordnungswidrigkeit ein.

Die mit dem Gesetz vorgenommene Ausweitung der Auskunftspflichten stellt aus Sicht des Datenschutzes eine deutliche Verschlechterung dar. Auskunftsmöglichkeiten von personenbezogenen Daten haben nunmehr nicht nur Strafverfolgungsbehörden und Gerichte wie nach dem TDDSG, sondern vielmehr alle Behörden, die zum Zweck der Strafverfolgung oder zur Gefahrenabwehr tätig werden, die Verfassungsschutzbehörden des Bundes und der Länder, der Bundesnachrichtendienst, der Militärische Abschirmdienst und alle Privaten in den Fällen, in denen dies zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist. Gerade die Privilegierung der Urheberrechteinhaber ist aus datenschutzrechtlicher Sicht sehr bedenklich. Es ist nicht nachvollziehbar, dass privatrechtliche Auskunftsansprüche mit den Rechten der Strafverfolgungsbehörden und der Polizei gleichgestellt werden. Wichtig ist es allerdings festzuhalten, dass die Regelungen im TMG nicht selbst die Anspruchsgrundlage für den Auskunftsanspruch sind, sondern lediglich klarstellen, dass etwaige Ansprüche nicht von vornherein durch Datenschutzbelange gesperrt sind. Es wäre stets eine die Datenerhebung legitimierende Rechtsgrundlage in einem Gesetz außerhalb des TMG erforderlich, wie z. B. der Strafprozessordnung oder dem Urhebergesetz. Eine solche Eingriffsgrundlage existiert lediglich im Bereich des Urheberrechts nicht.

5.2 Datenschutzbelange beim digitalen Fernsehen

Die Datenschutzbeauftragten des Bundes und der Länder beobachten schon seit geraumer Zeit die Pläne der privaten Fernsehveranstalter, ihre Angebote nur noch verschlüsselt zu übertragen. Hierbei werden vorrangig Geschäftsmodelle favorisiert, bei denen die kostenpflichtige Entschlüsselung des Signals nur mit personenbezogenen Smartcards möglich ist. Solche Pläne widersprechen dem im Rundfunkvertrag geltenden Gebot, dass die Inanspruchnahme von Rundfunk und deren Abrechnung anonym zu ermöglichen ist. Aus diesem Grund fordern die Datenschutzbeauftragten des Bundes und der Länder in einer auf der 73. Konferenz gefassten Entschließung, dass eine anonyme Nutzung auch bei zukünftigen digitalen Angeboten erhalten bleiben muss (vgl. Ziff. 21.1 dieses Berichts).

5.3 Bericht aus dem Arbeitskreis Medien

Der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zweimal im Jahr 2007 getagt. Dabei wurden gemeinsame Positionen erarbeitet und u. a. folgende Themen erörtert: Verfahren zur Befreiung der Rundfunkgebührenpflicht, datenschutzrechtliche Aspekte des Urheberrechts bei der Nutzung des Internets, anonyme Nutzung des Rundfunks, anonyme bzw. pseudonyme Nutzung von Foren durch Bedienstete der Verwaltung, Vorratsdatenspeicherung in der elektronischen Kommunikation und Ortung von Mobilfunkteilnehmern bei Notrufen.

6. Datenschutz durch Technikgestaltung und -bewertung

6.1 Übernahme Bremer Datenverarbeitungsverfahren durch Dataport

Mit Gesetz vom 20. Dezember 2005 trat das Land Bremen dem Länderstaatsvertrag zur Errichtung der Anstalt des öffentlichen Rechts Dataport bei. Dabei ging es zunächst um die Unterstützung der IT in der Steuerverwaltung (vgl. 28. JB, Ziff. 15.2). Im Jahr 2006 wurden in zwei Folgeprojekten die Weiterentwicklung des IT-Bereichs der bremischen Verwaltung und die Gründung einer bremischen Niederlassung des IT-Dienstleisters Dataport in Bremen behandelt und von mir begleitet (vgl. 29. JB, Ziff. 15.1). Mit Wirkung vom 1. Januar 2007 wurde der Eigenbetrieb fidatas Bremen auf die Anstalt öffentlichen Rechts Dataport übertragen, zu der auch fast alle ehemaligen Mitarbeiterinnen und Mitarbeiter der ID-Bremen gehören. Damit verbunden war die Standortverlagerung der Rechenzentrumsproduktion für die Freie Hansestadt Bremen vom Rechenzentrum ID-Bremen zu Dataport. Dataport wurde damit zum zentralen IT-Dienstleister der Freien Hansestadt Bremen. Eine Vielzahl von Verfahren, in denen z. T. sensible personenbezogene Daten verarbeitet werden, wurden nach Dataport migriert. Als Auftragnehmer muss Dataport deshalb durch geeignete technische und organisatorische Maßnahmen ein der Sensibilität der Daten angemessenes hohes Datenschutzniveau gewährleisten.

Diese Anforderungen galten auch für den Prozess der Migration. Ich formulierte daher, nachdem Dataport den Projektplan für die Durchführung vorgestellt hat, gegenüber der Senatorin für Finanzen bereits im Februar 2007 erste datenschutzrechtliche Anforderungen. Im Projektplan fehlten Termine für die Definition technischer und organisatorischer Maßnahmen, die für den datenschutzgerechten Ablauf der Migration erforderlich gewesen wären. Da Dataport Zugriffsberechtigungen zur Erledigung verschiedener Aufgaben benötigte, forderte ich die Dokumentation der Berechtigungsvergabe und des Umfangs einzelner Berechtigungen. Das Rechtemanagement sollte revisionssicher sein. Außerdem hielt ich es für erforderlich, das Verfahren zur Gewährleistung eines sicheren und vollständigen elektronischen und/oder physikalischen Transports, wozu auch die permanente Anbindung des Standortes Bremen an Hamburg gehört, zu dokumentieren. Darüber hinaus forderte ich Testkonzepte für die Durchführung der Tests und die Festlegung der für den während des Migrationsprozesses vergebenen administratorischen Rechte. Da die IT-Sicherheitsrahmenbedingungen in der Regel Einfluss nehmen auf die Sicherheit einzelner Verfahren, forderte ich ein Sicherheitskonzept von Dataport. Im April 2007 erinnerte ich das zuständige Referat bei der Senatorin für Finanzen noch einmal an die Erstellung der ausstehenden Dokumentation und an seine Pflicht als Generalauftraggeber, gem. § 9 BremDSG einen schriftlichen Auftrag an Dataport für die Auftragsdatenverarbeitung mit der Festlegung u. a. der technischen und organisatorischen Maßnahmen nach § 7 BremDSG zu erteilen. Aufgrund dieses Auftrags ist dann eine effektive Auftragskontrolle nach § 7 Abs. 4 Satz 2 Nr. 6 BremDSG zu gewährleisten. Auch diese Erinnerung blieb unbeantwortet, so dass mir bis heute keinerlei Aussage darüber möglich ist, auf welchem Datenschutzniveau die Migration abgelaufen ist.

Das Problem fehlender Informationen zum Sicherheitsmanagement und zur Sicherheitsarchitektur bei Dataport ist nicht nur auf die Migrationsphase beschränkt.

Bereits vor dem Beitritt zu Dataport hatte die Freie Hansestadt Bremen Dataport den Auftrag zur Unterstützung der IT-Steuerverwaltung im Rahmen eines sogenannten Datacenter Steuern erteilt. Meine Forderungen nach einem Test- und Migrationskonzept sowie einem Sicherheitskonzept (und

der Dokumentation von Berechtigungen) sind nicht erfüllt worden. In einer im Frühjahr 2007 in Hamburg für die beteiligten Länder stattfindenden Informationsveranstaltung sagte Dataport zu, dass die Arbeiten am Sicherheitskonzept bis zur Aufnahme des Produktionsbetriebs abgeschlossen sein werden. Der Produktionsbetrieb ist bereits im Herbst 2007 angelaufen, das Sicherheitskonzept wurde nun für Dezember d. J. angekündigt. Auch die dem Vertrag zwischen dem Land Bremen und Dataport über die Beschaffung von IT-Dienstleistungen beigefügten Anlagen und Serviceschein beschreiben lediglich allgemeine Sicherheitsziele. Festgelegt sind darin aber auch Kontrollrechte des Auftraggebers und die Verpflichtung von Dataport zur Erstellung eines Konzeptes zur Wahrung des Steuergeheimnisses, des Datenschutzes und der IT-Sicherheit (Sicherheitskonzept). In dem Konzept sollen einzelne technische, organisatorische, infrastrukturelle und personelle Maßnahmen sowie das verbleibende Restrisiko beschrieben werden. Die Erforderlichkeit dieser Konzepte wird demnach grundsätzlich akzeptiert. Die Konzepte konnten auf Nachfrage nicht vorgelegt werden, die Möglichkeit der Ausübung von Kontrollrechten ist deshalb nur sehr eingeschränkt möglich. Ergänzend sollten auch die Kontrollpflichten des Auftraggebers definiert werden, um deren Wahrnehmung zu garantieren.

Genau diese Festlegungen sind auch für andere Verfahren erforderlich. Die Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales gab mir ein Datenschutzkonzept für ein Verfahren zur Unterstützung der Sachbearbeitung im Bereich des Sozialdienstes junger Menschen, der Jugendgerichtshilfe und der wirtschaftlichen Hilfe zur Kenntnis. Mit dem Verfahren werden Daten verarbeitet, die beruflichen Schweigepflichten unterliegen und vom Sozialgeheimnis geschützt werden. Dieses Verfahren soll von Dataport betreut werden. Zur Bewertung der Datenverarbeitung bei Dataport wurde ein Serviceschein (Leistungsbeschreibung Server Hosting) vorgelegt. Er beschrieb einige technische Sicherheitsmaßnahmen auf abstrakter Ebene, die keine Bewertung ermöglichten. Ich habe deshalb dem Sozialressort einen Fragebogen übersandt, der allerdings nur die unmittelbare Systemumgebung betrifft. Die datenschutzrechtliche Verantwortung des Ressorts erstreckt sich aber auch auf die Inhalte eines noch zu erstellenden Rahmenkonzeptes für ein IT-Sicherheitskonzepts Dataport insgesamt, soweit es sich auf das Verfahren des Jugendamtes auswirkt.

Momentan halte ich eine nach § 7 Abs. 4 Satz 2 Nr. 6 BremDSG erforderliche Auftragskontrolle für nicht durchführbar. Sie soll gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Diese Gewährleistung ist eine fundamentale Voraussetzung für die Wahrnehmung der datenschutzrechtlichen Verantwortung. Wie fundamental diese Voraussetzung ist, wurde deutlich, als im Oktober diesen Jahres vom Hamburger Datenschutzbeauftragten eklatante Sicherheitslücken bei Dataport festgestellt wurden. Die Auswirkungen auf die Sicherheit Bremer Daten waren und sind unklar. Ich habe mich deshalb mit Schreiben vom 13. November 2007 an die Senatorin für Finanzen gewandt und um folgende Informationen gebeten: Eine Beurteilung des Sachverhalts durch das Ressort als verantwortliche Stelle, eine Beschreibung der von Dataport eingeleiteten Sofortmaßnahmen sowie ob und wann das Sicherheitsmanagement des Ressorts über die Sicherheitsmängel informiert wurde.

Bis zum Redaktionsschluss habe ich keine Antwort erhalten. Aufgrund der bisher wahrgenommenen datenschutzrechtlichen Probleme halte ich es für dringend erforderlich, dem Datenschutz im Rahmen des Vertragsverhältnisses mit Dataport einen angemessenen Stellenwert zu geben. Insgesamt gibt es

für Dataport noch viel zu tun. Ich hoffe, der spezielle Datenschutzsachverstand aus Bremen wird genutzt, um die Entwicklung voranzutreiben.

6.2 Dataport: Zentraler Service Desk für Dataport Bremen

Neben den datenschutzrechtlichen Fragen im Zusammenhang mit der Verlegung des Rechenzentrums von der ID Bremen GmbH zu Dataport nach Hamburg (siehe auch vorgehenden Artikel) habe ich mich im Rahmen einer Arbeitsgruppe, dem auch Vertreter der Senatorin für Finanzen, des Gesamtpersonalrats und Dataport angehören, mit der Thematik des Zentralen Service Desks und den dort eingesetzten Produkten aus datenschutzrechtlicher Sicht auseinander gesetzt. Konkret geht es hier um den Einsatz eines Tools zur Fernwartung, eines Produktes zur Inventarisierung von Hard- und Software sowie eines so genannten Ticketmanagementsystems zur Aufzeichnung eingehender Aufträge (gemeldete Probleme) und deren Lösungen.

Fernwartung: Zum Einsatz einer Software für die Fernwartung von Arbeitsplätzen in der bremischen Verwaltung hat Dataport einen Service-Schein vorgelegt, in dem u. a. die technischen und organisatorischen Maßnahmen nach dem Bremischen Datenschutzgesetz beschrieben wurden. Das Produkt selbst habe ich mir vor Ort angesehen.

Meine Hauptforderungen für den datenschutzgerechten Einsatz einer Fernwartungssoftware sind die Verschlüsselung der Datenübertragung, die revisionssichere Protokollierung der Zugriffe durch die Fernwartungssoftware und die Schaffung von Transparenz für die Mitarbeiter der bremischen Verwaltung, auf deren Arbeitsplatz zugegriffen wird. In einer Arbeitsanweisung für die Service-Desk-Mitarbeiter sind Bedingungen, Vorgehensweise und Details zur Ausführung der Fernzugriffe dokumentiert und festgelegt worden.

Der Zugriff auf einen Arbeitsplatz durch einen Service-Desk-Mitarbeiter von Dataport darf nur auf konkrete Veranlassung durch einen Auftrag (Dokumentation im Ticketmanagement) und ausschließlich unter Einsatz des definierten Fernwartungstools erfolgen. Der Nutzer des Zielsystems muss dem Fernzugriff ausdrücklich durch eine auf dem Bildschirm zu bestätigende Anfrage zustimmen. Der Service-Desk-Mitarbeiter verfügt nach der Anmeldung über die gleichen Rechte wie der betroffene Mitarbeiter. Lehnt der Nutzer des Ziel-Systems die Verbindungsanfrage ab, wird keine Verbindung hergestellt.

Der Nutzer des Ziel-Systems hat die Fernwartungssitzung am Bildschirm zu verfolgen und verfügt über die technischen Mittel, die Sitzung bei Bedarf abzubrechen. Reichen die Rechte des Nutzers des Ziel-Systems nicht aus, um das Problem zu beheben, so ist auch für eine Anmeldung mit Administrationsrechten am Ziel-System eine Zustimmung durch den betroffenen Mitarbeiter erforderlich. Während der gesamten Fernwartung besteht ein Telefonkontakt zwischen dem betroffenen Mitarbeiter und dem Service-Desk-Mitarbeiter, der nur mit Einverständnis des Anwenders unterbrochen werden darf, wenn die Störungsbeseitigung länger als fünf Minuten dauert. Ein „Dunkel-Schalten“ des Bildschirms des Zielsystems ist unzulässig. Durch ein kleines Icon am Bildschirmrand wird die Verbindung des Zielsystems zum Service-Desk-Mitarbeiter angezeigt.

Die Aktivitäten zur Problembehebung werden durch den Service-Desk-Mitarbeiter im Servicemanagement dokumentiert. Es ist unzulässig, Screenshots oder Videosequenzen vom Bildschirm des Zielsystems zu erstellen.

Der Mitarbeiter des Service-Desk darf nicht unter einem Sammelbenutzer arbeiten, sondern muss eindeutig identifizierbar sein. Dies ist Voraussetzung für die von mir geforderte revisionssichere Protokollierung aller Zugriffe. Dessen Realisierung wurde mir bis zum 15. März 2008 zugesichert.

Ich bewerte die zur Fernwartungssoftware im Service-Schein beschriebenen technischen und organisatorischen Maßnahmen vorbehaltlich der Prüfung einiger nachgereichter Dokumente unter folgenden Voraussetzungen als angemessen:

- die Aktivierung einer revisionssicheren Protokollierung erfolgt fristgemäß,
- die Verschlüsselung der Datenübermittlung erfolgt mit dem nächsten Release und
- jeglicher administrativer Zugriff ohne Nutzung der Fernwartungssoftware ist nicht zulässig.

Inventarisierung von Hard- und Software: Über den Einsatz eines Softwarewerkzeugs zur Inventarisierung von Hard- und Software auf bremischen Arbeitsplätzen durch Dataport wurde ich ebenso wie der Gesamtpersonalrat nicht informiert. Erst durch seine Intervention bekam ich Kenntnis vom Einsatz dieses Produktes. Mitarbeiter hatten sich darüber beklagt, dass die Recherchevorgänge der Inventarisierungssoftware die Rechnerkapazitäten der Arbeitsplätze stark einschränkten.

Den Einsatz eines solchen Produktes hält Dataport für erforderlich, um stets einen aktuellen Überblick über die eingesetzte Hard- und Software (Inventarisierung) vorliegen zu haben. Bereits bei der Demonstration des Tools wurden allerdings einige Probleme deutlich, die von Bedeutung sind. So ist beispielweise die Eingriffsebene auf Dateiebene so tief, dass Dateien bis hin auf die Namensebene aufgelistet wurden, wodurch sich ein Rückschluss auf den Inhalt der Dateien ergeben kann. Eine Analyse der vorhandenen Daten in dieser Form und Tiefe ist für eine Inventarisierung nicht erforderlich.

Erschwerend tritt hinzu, dass undokumentiert ist, über welchen Funktionsumfang das ausgewählte Programm insgesamt verfügt, in welcher Weise sich der Funktionsumfang konfigurieren und reduzieren lässt und wie Änderungen an den noch zu vereinbarenden Konfigurationen revisionssicher protokolliert werden können.

Weitere Informationen dazu sollten mir bis Anfang November vorgelegt werden, sind aber bis Redaktionsschluss nicht eingegangen. Zwischenzeitlich wurde mir mitgeteilt, dass eine interne Prüfung zur Revisionssicherheit bei Dataport ergeben hat, dass die Anforderungen an das Tool mit hoher Wahrscheinlichkeit nicht mit entsprechenden Features hinterlegt sind, möglicherweise aber auf den Einsatz der Inventarisierungssoftware ganz verzichtet werden kann.

Ich erwarte nun eine abschließende Klärung des Funktionsumfangs, der Konfigurations- und Protokollierungsmöglichkeiten des Tools bzw. eine verlässliche Aussage darüber, ob die Nutzung dieser Software komplett entfällt.

Auftragsmanagementsystem: Über das so genannte Ticketmanagement (Verwaltung von Serviceaufträgen) werden eingehende Problemmeldungen beispielweise zu Office-Produkten, zu Druckern und zum E-Mail-Verkehr durch den Service-Desk aufgenommen und durch zuständige Mitarbeiter bei Dataport bearbeitet. Dabei werden die betroffenen Mitarbeiter der bremischen Verwaltung über das Ticketsystem und daraus resultierende E-Mails über den Bearbeitungsstand ihrer Problemmeldung (Ticket) informiert.

Zu diesem Produkt liegt mir zwar ebenfalls ein Service-Schein vor, allerdings sind hier die technischen und organisatorischen Maßnahmen unvollständig und nicht ausreichend beschrieben. Ich habe hierzu weitere Angaben angefordert.

6.3 Zentrale Protokollierung der Internet-Nutzung der bremischen Verwaltung

Die meisten Arbeitsplätze in der bremischen Verwaltung haben einen Internetzugang. Dies ist mittlerweile ein unentbehrliches Hilfsmittel, um die Aufgaben effektiv zu erledigen. Neben der dienstlichen Nutzung ist es den Beschäftigten in geringem zeitlichen Umfang erlaubt, den Zugang privat zu nutzen. Beide Arten der Nutzung werden an zentraler Stelle bei der BREKOM, die das Bremische Verwaltungsnetz (BVN) und den zentralen BVN-Dienst „Internet-Zugang“ betreibt, protokolliert. Verantwortliche Stelle für die Protokollierung ist die Senatorin für Finanzen. Grundlage der Protokollierung ist die im Amtsblatt 2004-20 der Freien Hansestadt Bremen veröffentlichte „Richtlinie für die Bereitstellung und Nutzung von Internet/Intranet-Zugängen“ (Näheres vgl. 26. JB, Ziff. 1.3).

Die Protokollierung dienstlicher und privater Internet-Aktivitäten habe ich im Spätherbst einer Datenschutzprüfung unterzogen. Dabei habe ich u. a. das Folgende festgestellt.

Die Senatorin für Finanzen und die BREKOM unterscheiden bei der Erhebung von Nutzungsdaten zwischen so genannten Log-Daten und Protokolldaten. Dabei sind Log-Daten (Logs, Log-Dateien) die vollständigen Nutzungsprotokolle. Bei dienstlicher Nutzung sind die vollständigen IP-Adressen des jeweils aktuellen Tages in den Log-Daten enthalten. Bei privater Nutzung wird gleich beim Schreiben des Logs die jeweilige IP-Adresse auf Null gesetzt. Logs werden tageweise geschrieben.

Protokolldaten sind Log-Dateien, in denen die vollständigen IP-Adressen um die letzten drei Stellen gekürzt sind und damit lediglich Rückschlüsse auf das jeweilige Netzsegment, aus dem die Anfragen stammen, zulassen. Einmal täglich werden die Logs automatisiert in Protokolle gewandelt („Rotation“). Die ursprüngliche Log-Datei mit den vollständigen IP-Adressen liegt nach der Rotation im System nicht mehr vor.

Zum Zeitpunkt der Prüfung musste ich allerdings feststellen, dass bei Logs und auch Protokollen auf dem Proxy (Server für die private Nutzung) die vollständige IP-Adresse des Rechners innerhalb des BVN protokolliert wurde, von dem die jeweiligen Anfragen stammten. Dies steht in Widerspruch zur vorgenannten verabschiedeten Richtlinie und stellt zugleich einen Verstoß gegen das Telemediengesetz (TMG) dar. Die unzulässigen Protokolldateien waren zum Zeitpunkt der Prüfung maximal drei Wochen alt. Dazu wurde mir berichtet, dass drei Wochen vor meinem Prüftermin der Proxy-Server für die private Internet-Nutzung neu installiert werden musste und dass versehentlich sowohl das Regelwerk für die dienstliche Nutzung eingestellt als auch die Rotation nicht entsprechend der obigen Beschreibung angepasst und kontrolliert wurde. Die Mitarbeiter der BREKOM haben in meinem Beisein die fehlerhaften Log- und Protokolldateien „rotiert“ und die IP-Adresse auf die Netzadresse der Anfrage reduziert. In meinem Prüfbericht habe ich verlangt, dass die Entstehung des Fehlers genau untersucht und mir nachgewiesen wird, wie zukünftig derartige Fehlkonfigurationen vermieden werden sollen. Weitere Abweichungen zu Richtlinie und TMG habe ich nicht festgestellt.

6.4 Datenschutzgerechte Entsorgung von optischen und magnetischen Datenträgern

In seiner Pressemitteilung „Sammlung von alten CDs in Bremen ein Riesenerfolg“ vom 2. Mai 2007 hat der Senator für Bau, Umwelt und Verkehr (SBUV) über die erfolgreiche Sammlung von Alt-CDs bei den Recycling-Stationen hingewiesen. In der Pressemitteilung hat er den Tipp gegeben, alte CDs mit sensiblen Daten mittels eines Kratzers auf der lesbaren Seite unbrauchbar zu machen. Mit dieser Methode ist aber keineswegs sichergestellt, dass die Datenträger dadurch irreversibel unbrauchbar gemacht wurden und damit die Daten unumkehrbar vernichtet sind.

Problematisch sehe ich dies beispielsweise insbesondere im Bereich von Arztpraxen oder Rechtsanwaltskanzleien, die aufgrund der kleinen Mengen anfallender Daten auf optischen Datenträgern keine spezielle Entsorgungsfirma für die datenschutzgerechte Entsorgung der Datenträger nutzen. Gleiches gilt für viele andere Berufsfelder und besonders auch Bürgerinnen und Bürger, die sensible private Daten auf optischen Datenträgern gespeichert und keine andere Möglichkeit haben, diese datenschutzgerecht zu entsorgen.

Bei optischen Datenträgern (CD, DVD) versagt die bei magnetischen Datenträgern leicht einzusetzende Methode des Löschens der Daten durch (mehrfaches) Überschreiben mit zufälligen Zeichenfolgen (nähere Informationen dazu unter http://www.datenschutz-bremen.de/pdf/oh_sicheres_loeschen.pdf). Eine physikalische Datenlöschung auf optischen Datenträgern ist in der Regel nur dann sichergestellt, wenn der Datenträger etwa durch Verbrennung, Zermahlen oder Einschmelzen zerstört wird. Je nach Sensibilität der Daten reicht ein Zerbrechen des Datenträgers in wenige grobe Stücke nicht für eine datenschutzgerechte Entsorgung aus. Sie sind für Spezialisten immer noch rekonstruierbar. Ein einzelner Kratzer ist selbst für Laien kein großes Hindernis. Teile der Daten können meist einfach auf andere Datenträger kopiert werden. Durch Einsatz von CD- und DVD-Reparatursets und durch Entfernung der Kratzer kann möglicherweise sogar der gesamte Datenbestand wieder hergestellt werden. Weitere Informationen zum Thema „Löschung und Datenträgervernichtung“ habe ich unter www.datenschutz-bremen.de/pdf/datenloeschung.pdf zusammengestellt.

Weiter zu bedenken ist: Die große Unsicherheit für den Eigentümer der Daten ist der Zeitraum zwischen Abgabe der CDs bei den Recycling-Stationen und der Verarbeitung durch eine Recycling-Firma. Es ist nicht abschließend sichergestellt, dass in der Zwischenzeit Daten unbefugt gelesen oder kopiert werden können.

Die umweltgerechte Entsorgung bzw. Recycling von CD und DVD ist erforderlich. In Bremen könnte die Vernichtung von optischen Datenträgern mit sensiblen Daten als besondere Dienstleistung angeboten werden. Um das Verfahren datenschutzgerecht auszugestalten, sollte der SBUV aber entsprechende Vorkehrungen treffen. Zu denken wäre zum einen, dass an zentraler Stelle, z. B. Recyclinghöfen, ein Schredder aufgestellt wird, in dem die Datenträger von dem Anliefernden unmittelbar selbst vernichtet werden können. Zum anderen wäre das Aufstellen von eingriffs- und entwendungssicheren Gefäßen mit der öffentlichen Zusicherung einer datenschutzgerechten Entsorgung. Dies habe ich dem SBUV vorgeschlagen, eine Antwort habe ich noch nicht erhalten.

6.5 Bericht aus dem Arbeitskreis Technik

Ich beteilige mich regelmäßig an dem AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Zentrale Themen waren u. a. die technischen Aspekte der Online-Durchsuchung. Hier hat der AK Technik für die Konferenz der Datenschutzbeauftragten ein Papier mit den technischen Aspekten der geplanten Online-Durchsuchung erarbeitet.

Zu dem Thema „Auswertetools für Protokolldateien“ haben nach Erfahrung der Datenschutzbeauftragten des Bundes und der Länder die Betreiber elektronischer Verfahren häufig keine revisionsfähigen und unvollständigen Protokollrohdaten, auch Werkzeuge zur Auswertung dieser Daten fehlen sehr oft. Im AK Technik wird derzeit ein Papier mit Anforderungen an Protokollierungssysteme formuliert, um den Verfahrensbetreibern entsprechende Informationen über die Ausgestaltung einer datenschutzgerechten Protokollierung an die Hand zu geben.

Ein weiteres Thema sind das IT-Sicherheits- und Datenschutzmanagement. Datenschutz- und IT-Sicherheits-Management haben in sehr vielen Fällen deckungsgleiche Ziele, die es durch strukturierte und standardisierte Organisation und Umsetzung beider Seiten zu nutzen gilt.

6.6 E-Government und Grundsatzfragen der Verwaltungsmodernisierung

Der Arbeitskreis Grundsatzfragen der Verwaltungsmodernisierung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschäftigte sich mit der revisionssicheren Langzeitarchivierung elektronischer Dokumente, den datenschutzrechtlichen Anforderungen bei der Umsetzung der EU-Dienstleistungsrichtlinie 2006/123/EG, Problemen bei Web-Auftritten öffentlicher Stellen, die im Rahmen einer Orientierungshilfe erläutert werden sollen, Fragen der Geodatenverarbeitung und der Auftragsdatenverarbeitung, Problemen von sog. Ratsinformationssystemen und schließlich datenschutzrechtlichen Anforderungen an ePayment-Verfahren und den Betrieb der Landesportale, wie es www.bremen.de darstellt.

7. Bremische Bürgerschaft – Medienausschuss / Datenschutz

Der Datenschutz, der in der letzten Legislaturperiode vom Rechtsausschuss begleitet wurde, ist nun dem „Ausschuss für Informations- und Kommunikationstechnologien und Medienangelegenheiten“ – kurz dem Medienausschuss - zugeordnet. Da der Ausschuss auch für die Informationsfreiheit zuständig ist, hat er einen Überblick über alle Aufgaben meiner Dienststelle. Mit dem Ausschuss ist eine Konzentration bei der Behandlung der Themen verabredet.

Eingangs möchte ich hervorheben, dass ich die Überlegungen des Ausschusses unterstütze, das Verfahren zur Behandlung meiner Jahresberichte zu beschleunigen. Denn es ist für die Behandlung nicht förderlich, ja ein Stück weit wirkungslos, wenn – wie jetzt geschehen - erst im Jahr 2008 in der Bremischen Bürgerschaft über Dinge gesprochen wird, die sich bereits im Jahr 2006 ereignet haben. Ich beabsichtige, dem Ausschuss weitere Vorschläge zu unterbreiten, um das Verfahren zu straffen, um so eine zeitnahe Behandlung der Themen des Berichts im Ausschuss und im Parlament zu ermöglichen.

Der Ausschuss hat unmittelbar nach der Sommerpause die Behandlung des 29. Jahresberichts und der Stellungnahme des Senats in Angriff genommen und sah sich gleich mit Altlasten aus der letzten Legislaturperiode konfrontiert. Ein Stück weit reifte dabei die Erkenntnis, dass einige Verwaltungszweige bei der Umsetzung des Datenschutzes sich im Schneckentempo bewegen. Als Ergebnis seiner zügig durchgeführten Beratungen legte der Ausschuss seinen Bericht an das Parlament bereits am 26. November 2007 vor, den ich im Folgenden wiedergebe.

7.1 Ergebnisse der Beratungen des 29. Jahresberichts

Bericht und Antrag des Ausschusses für Informations- und Kommunikationstechnologie und Medienangelegenheiten zum 29. Jahresbericht des Landesbeauftragten für den Datenschutz vom 31. März 2007 (Drucksache 16/1362) und zur Stellungnahme des Senats vom 28. August 2007 (Drucksache 17/31)

Bericht

Die Bürgerschaft (Landtag) überwies in ihrer Sitzung am 11. Juli 2007 den 29. Jahresbericht des Landesbeauftragten für den Datenschutz vom 31. März 2007 (Drucksache 16/1362) und in ihrer Sitzung am 19. September 2007 die dazu erfolgte Stellungnahme des Senats vom 28. August 2007 (Drucksache 17/31) an den Ausschuss für Informations- und Kommunikationstechnologie und Medienangelegenheiten zur Beratung und Berichterstattung.

Der Ausschuss nahm seine Beratungen in seiner Sitzung am 21. September 2007 auf und stellte bei den nachfolgend aufgeführten Punkten Beratungs- und Handlungsbedarf fest:

1. Ergebnisse der Beratungen des 28. Jahresberichts im Rechtsausschuss (Ziffer 7.1) – Telekommunikationsüberwachung,
2. Rahmendatenschutzkonzept und andere Verfahren beim Stadtamt Bremen (Ziffer 9.19),
3. Datenverarbeitungsverfahren Fundinfo (Ziffer 9.21),
4. Anbindung der Amtsgerichte und Staatsanwaltschaft an das BZR (Ziffer 10.1).

Der Ausschuss erörterte die genannten Komplexe mit dem Landesbeauftragten für den Datenschutz in seinen Sitzungen am 21. September und, unter Hinzuziehung der Vertreter des Senators für Inneres und Sport sowie des Senators für Justiz und Verfassung, am 19. Oktober 2007.

Zu den einzelnen Punkten nimmt der Ausschuss für Informations- und Kommunikationstechnologie und Medienangelegenheiten wie folgt Stellung:

a) Ergebnisse der Beratungen des 28. Jahresberichts (Ziffer 7.1) – Telekommunikationsüberwachung: Im Rahmen der Beratungen zum 28. Jahresbericht war bereits dem Rechtsausschuss dargelegt worden, dass schon die Prüfung der Telekommunikationsüberwachung der Polizei durch den Landesbeauftragten für den Datenschutz im Jahre 2004 technische und organisatorische Mängel offenbarte, die in der Folgezeit nicht behoben wurden. Der Rechtsausschuss wurde im Herbst 2005 befasst. Ihm wurde dann bei der Beratung des 28. Jahresberichts vom Senator für Inneres und Sport zugesagt, das erforderliche Datenschutzkonzept für die Komponenten des Systems der Telekommunikationsüberwachung bis Ende Februar 2006 vorzulegen. Es lag dann erst zum Juli 2006 vor und enthielt weiterhin Defizite. Zum Ende August 2007 lag eine angepasste Verfahrensbeschreibung vor, in der einige Mängel behoben worden waren.

Weiterhin problematisch ist die fehlende Zugriffs- und Eingabekontrolle der Verschriftungssoftware TÜPFO. Der Senator für Inneres und Sport legte dar, dass diese Software ohne Abstriche für ihre Einsatzfähigkeit nicht umgestaltungsfähig sei und kündigte die Umstellung auf eine neue Software an, die Mitte 2009 betriebsfähig sein werde.

Der Ausschuss für Informations- und Kommunikationstechnologie und Medienangelegenheiten nimmt zur Kenntnis, dass der Senator für Inneres und Sport auf ein neues System umstellen wird, das nach seiner Auffassung die Anforderungen des Datenschutzes nach den Hinweisen des Landesbeauftragten für Datenschutz und Informationsfreiheit berücksichtigt.

Der Ausschuss fordert den Senator für Inneres und Sport auf, Gespräche mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit zu führen, um im gegenwärtigen System für die Übergangszeit bis Mitte 2009 ohne erhebliche Mehrkosten eine Lösung herbeizuführen, die den Anforderungen des Datenschutzes gerecht wird.

Der Ausschuss bittet den Landesbeauftragten für Datenschutz und Informationsfreiheit um einen Zwischenbericht im Januar 2008.

b) Rahmendatenschutzkonzept und andere Verfahren beim Stadtamt Bremen (Ziffer 9.19): Der Rechtsausschuss hatte sich bereits im Jahr 2006 mehrfach mit den seit mehreren Jahren beim Stadtamt Bremen zu verschiedenen DV-Verfahren ausstehenden Fachdatenschutzkonzepten und dem fehlenden Rahmendatenschutzkonzept beschäftigt und hierzu der Bremischen Bürgerschaft zum 28. Jahresbericht berichtet.

Das Rahmendatenschutzkonzept wurde im Januar 2007 vorgelegt und die verbliebenen Kritikpunkte im April 2007 im Rechtsausschuss behandelt. Mit dem Stadtamt wurde seitens des Landesbeauftragten für Datenschutz und Informationsfreiheit eine Prioritätenliste vereinbart, in der unter anderem spezielle Regelungen für die besonderen Sicherheitsbereiche Rechenzentrum, Kommunikationstechnik und Datenträgerarchiv, für Rollenkonzepte auf Netzwerkebene, Berechtigungskonzepte auf Verzeichnisebene und Administrationskonzepte aufgeführt sind.

Der Ausschuss für Informations- und Kommunikationstechnologie und Medienangelegenheiten nimmt zur Kenntnis, dass bis September 2008 ein neues Konzept des Stadtamtes in Abstimmung mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit erstellt werden soll.

Der Ausschuss bittet um einen Zwischenbericht im Januar 2008 mit Bewertung beider Seiten.

c) Datenverarbeitungsverfahren Fundinfo (Ziffer 9.21): Die datenschutzrechtlich relevanten Dokumente sind noch nicht im Sinne der Stellungnahme des Landesbeauftragten für Datenschutz und Informationsfreiheit vom November 2006 angepasst worden. Der Senator für Inneres und Sport erklärte, dass nunmehr eine Anpassung im November 2007 erfolgt.

Der Ausschuss für Informations- und Kommunikationstechnologie und Medienangelegenheiten nimmt den Sachstand zur Kenntnis und bittet den Landesbeauftragten für Datenschutz und Informationsfreiheit um einen bewertenden Bericht im Januar 2008.

d) Anbindung der Amtsgerichte und Staatsanwaltschaft an das BZR (Ziffer 10.1)

Der Ausschuss für Informations- und Kommunikationstechnologie und Medienangelegenheiten nimmt zur Kenntnis, dass zwischen dem Landes-beauftragten für Datenschutz und Informationsfreiheit und dem Senator für Justiz und Verfassung Einvernehmen hergestellt wurde, und die Verwaltungsvereinbarung mit Niedersachsen im Sinne des Vorschlags des Landesbeauftragten für Datenschutz und Informationsfreiheit ergänzt werden soll.

Der Ausschuss bittet um einen Sachstandsbericht im Januar 2008.

II. Antrag

Die Bürgerschaft (Landtag) möge beschließen:

Die Bürgerschaft (Landtag) tritt den Bemerkungen des Ausschusses für Informations- und Kommunikationstechnologie und Medienangelegenheiten bei.

7.2 Weitere Themen im Ausschuss und im Parlament

Die Bürgerschaft (Landtag) hat noch Ende der letzten Legislaturperiode das Bremische Schuldatenschutzgesetz - BremSchulDSG (BremGBl. 2007, S. 187) verabschiedet, das ich intensiv datenschutzrechtlich beraten habe, wie auch das Gesetz zur Sicherung des Kindeswohls und zum Schutz vor Kindesvernachlässigung (Kindeswohlgesetz – KiWG) (BremGBl. 2007, S. 317) verabschiedet, das ebenfalls eine Reihe von Datenverarbeitungsvorschriften enthält, zu denen ich Stellung genommen habe. Ebenfalls dazu zählt das Jugendstrafvollzugsgesetz (BremGBl. 2007, S. 233). Näheres dazu vgl. Ziff. 10.3 dieses Berichts.

Neben der Verabschiedung von Gesetzen mit datenschutzrechtlichen Regelungen hat sich die Bürgerschaft (Landtag) zum Beispiel mit einem Antrag beschäftigt, der den Bremer Senat auffordert, die Einrichtung einer öffentlich einsehbaren Kartei von Sexualtätern vorzunehmen (vgl. Drs. 17/29). Der genannte Antrag wurde von allen Fraktionen in der Bürgerschaft (Landtag) abgelehnt. Ich wurde vom Senat zuvor um eine Stellungnahme gebeten und habe erhebliche datenschutzrechtliche Bedenken geäußert. Auch die 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis. 9. März 2007 in Erfurt hat in einer Entschließung solche Pläne bezüglich einer allgemein zugänglichen Straftäterdatei für verfassungswidrig erklärt (vgl. Ziff. 21.3 dieses Berichts).

Auch die Durchführung der beiden Untersuchungsausschüsse gab für mich reichlich Anlass, sich mit Fragen des Datenschutzes zu beschäftigen. So ging es um Fragen des Umgangs mit dem gesamten E-Mail-Verkehr der beiden Sekretärinnen des Klinikgeschäftsführers oder aber die Auswahl und Zurverfügungstellung von Vergleichsakten im Fall Kevin.

Besonders positiv habe ich die durch eine große Anfrage eingeleitete Debatte zur Entwicklung und den Einsatz von RFID-Tags, der Funkchiptechnologie wahrgenommen (vgl. Drs. 16/1312). Darin wurde deutlich, dass neben dem ungeheueren wirtschaftlichen Potential, das in dieser Entwicklung steckt, auch die datenschutztechnischen Risiken gesehen wurden. Denn es gilt der Gefahr zu begegnen, dass RFID, Biometrie und ubiquitäres Computing zur Überwachung des Einzelnen führt. Wenn der Einzelne mit diesen Mitteln jederzeit lokalisierbar und identifizierbar wird, könnte er davor zurückschrecken, die ihm zustehenden Grundrechte wie Demonstrations- oder Meinungsfreiheit in Anspruch zu nehmen. In der Bürgerschaftsdebatte wurde deutlich, dass alle Fraktionen das Thema weiter verfolgen und sich dafür einsetzen wollen, dass das Recht auf Privatsphäre und informationelle Selbstbestimmung auch mit der RFID-Technologie gewahrt bleibt. Die Antwort des Senats erfolgte am 10. April 2007 (vgl. Drs. 16/1368). In der 83. Sitzung der Bürgerschaft (Landtag), am 26. April 2007 wurde das Thema hinreichend debattiert (vgl. PlPr. S. 5638 ff.).

7.3 Veröffentlichung personenbezogener Daten einer Drucksache der Bremischen Bürgerschaft im Internet

Eine Petentin beschwerte sich bei mir, dass die in einer Drucksache der Bremischen Bürgerschaft aus dem Jahre 2004 enthaltenen Vorschlagslisten für die Wahl ehrenamtlicher Richter am Verwaltungs- und Oberverwaltungsgericht im Internet veröffentlicht worden waren. Durch „googeln“ ihres Namens gelangte man als einzigen Sucheintrag auf die Drucksache, in der sich neben dem Namen der Petentin u. a. auch das Geburtsdatum und die Adresse befanden. Eine öffentliche Bekanntgabe dieser Daten hatte die Petentin als ehrenamtliche Richterin zu vermeiden gesucht, damit nicht Parteien aus Gerichtsverfahren, an denen sie öffentlich mitwirkt, sie zuhause aufsuchen oder belästigen.

Ich wandte mich an die senatorische Dienststelle, welche die Drucksache erstellt hat, und parallel an die Verwaltung der Bremischen Bürgerschaft, um zu klären, auf welche Weise die personenbezogenen Daten ins Internet gelangt sind. Auf Seiten der erstellenden senatorischen Dienststelle konnte ich keine Fehler ausmachen. Die Drucksache sah vor, dass die personenbezogenen Daten nicht in die veröffentlichte und dann ins Internet eingestellte Drucksache aufgenommen werden. Diese mit mir in der Vergangenheit ausgehandelte Vorgehensweise hatte vorliegend allerdings nicht funktioniert. Im Ergebnis entfernte die Bremische Bürgerschaft auf meine Hinweise hin die Verlinkung zu der Drucksache, so dass diese auch über Suchmaschinen nicht mehr angezeigt wurde. An welcher Stelle bei der Verwaltung der Bremischen Bürgerschaft das Büroversehen im Jahre 2004 entstanden war, ließ sich nicht mehr aufklären. Auch ist das technische Verfahren zur Veröffentlichung gegenüber dem Jahre 2004 mittlerweile sicherer geworden. Im Ergebnis lassen sich die fraglichen Daten der Petentin über eine einfache Suchmaschinenfunktion im Internet aus der Drucksache nicht mehr feststellen.

8. Personalwesen

8.1 Keine Aufzeichnung von Telefongesprächen zur Störungsbeseitigung in der TK-Anlage der Bremischen Verwaltung

Im Zuge der Einführung einer neuen Telekommunikationsanlage in der bremischen Verwaltung sind sporadische Störungen bzw. Fehler aufgetreten, z. B. waren Worte oder einzelne Wortsilben für den anderen Gesprächspartner nicht oder nur schwer verständlich und es wurden wechselnde Lautstärken während der Gespräche festgestellt. Die Fehler lassen sich weder reproduzieren noch auf einen bestimmten Teilnehmerkreis einschränken. Der Diensteanbieter hatte erklärt, als einzige Möglichkeit bliebe nur eine Aufzeichnung der betreffenden Telefongespräche, um im zeitlichen Kontext mit den Verbindungsdaten die Ursache der Störung ausfindig zu machen. In anderen Bundesländern würde auch so verfahren. Allerdings könne er nicht ausschließen, dass auch diese Methode nicht zum Erfolg führe. Weil durch eine Aufzeichnung der Telefongespräche die Inhaltsdaten der Gesprächsteilnehmer (Beschäftigte, Bürger u. a.) und damit das Telekommunikationsgeheimnis tangiert seien, hatte die Senatorin für Finanzen angefragt, ob die Aufzeichnung zulässig ist.

In meiner Antwort habe ich erklärt: § 100 Abs. 1 Telekommunikationsgesetz (TKG) regelt präzise und abschließend, dass zur Beseitigung von Störungen und Fehlern nur Bestands- und Verbindungsdaten erhoben und verarbeitet werden dürfen. Demzufolge ist die Aufzeichnung von Telefongesprächen ohne wirksame Einwilligung aller betroffenen Gesprächspartner nicht zulässig.

Weil behauptet wurde, auch in anderen Bundesländern werde so verfahren, habe ich mich an die Datenschutzbeauftragten des Bundes und der anderen Länder gewandt. Diese unterstützen meine Rechtsauffassung einhellig.

8.2 Personaldaten aus Untersuchungsbericht im Internet

Die Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales hatte einen Sonderermittler beauftragt, das Geschäftsgebaren des ehemaligen Chefs des Klinikums Bremen-Ost zu untersuchen. Der von dem Untersuchungsführer erstellte vielseitige Bericht enthält eine ganze Reihe von personenbezogenen Angaben über den Klinikchef, beginnend mit dessen Bewerbung und anderen Daten über das Beschäftigungsverhältnis, die nur der Personalakte entnommen sein können. Dieser Bericht wurde nicht nur in Gänze der Presse zur Verfügung gestellt, sondern darüber hinaus vom Ressort noch im Internet veröffentlicht. Ich wurde durch einen Zeitungsartikel darauf aufmerksam und habe mich umgehend an die Senatorin gewandt und um Stellungnahme gebeten. Auf meine Anfrage hat die Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales mitgeteilt, dieser Sachverhalt sei zutreffend. Nach einer Beschwerde des Betroffenen sei der Bericht aus dem Netz genommen worden.

Selbstverständlich müssen sich öffentliche Stellen, wenn ihnen Misswirtschaft oder Fehlverhalten vorgeworfen werden, auch öffentlich wehren und zu den Vorwürfen Stellung nehmen können. Es ist jedoch unzulässig, wenn öffentliche Stellen dabei mehr oder weniger großzügig Informationen aus dem Beschäftigungsverhältnis von Betroffenen der Öffentlichkeit preisgeben, ohne dass diese in einem unmittelbaren Zusammenhang mit den Vorwürfen stehen, die aufzuklären sind. Auch wenn der politische Druck in der Öffentlichkeit groß ist, hätte ich erwartet, dass das Ressort den Untersuchungsbericht des Sonderermittlers auswertet und nur die Tatsachen der Öffentlichkeit preisgibt, die zur Aufklärung der öffentlich Vorwürfe erforderlich sind.

9. Inneres

9.1 Videoüberwachung in Polizeifahrzeugen

Die Polizei Bremen hat derzeit 12 von 45 Fahrzeugen mit Videogeräten ausgestattet, die das Vorgehen der Beamten bei Anhalte- und Kontrollvorgängen im öffentlichen Verkehrsraum aufzeichnen. Ich wurde darüber im September diesen Jahres informiert. Es handelt sich hier um Videodaten zur Eigensicherung nach § 29 Abs. 5 Bremisches Polizeigesetz (BremPolG), d. h. um Leib und Leben der Polizeibeamten zu sichern.

Die Polizei Bremen legte mir eine entsprechende Dienstanweisung vor, die die Einzelheiten zur Ausführung des § 29 Abs. 5 BremPolG regelt. Ich habe mir die Datenverarbeitung vor Ort angesehen.

Die Aufzeichnung beginnt bei Einschalten der Anhaltebrücke mit dem „Stopp Polizei"-Signal oder durch manuelle Betätigung einer Bedientaste. Die Aufzeichnung endet nicht automatisch, sondern erst wieder bei Betätigung einer Bedientaste. Der Aufnahmebetrieb im Fahrzeug wird durch ein optisches Signal (rote Kontrollleuchte) angezeigt.

Der Betroffene soll, da es sich um eine Maßnahme mit Präventionscharakter handelt, die Angriffe verhindern soll, zusätzlich auf die Aufzeichnung hingewiesen werden. Auf Nachfrage soll Betroffenen und Dritten mitgeteilt werden, dass eine unverzügliche Löschung der Daten stattfindet, wie sie auch das Bremische Polizeigesetz vorsieht. Tatsächlich aber werden die Daten erst nach zwölf Stunden gelöscht bzw. überschrieben.

Eine Auswertung der Speicherkarten und Speicherung der Videodaten auf CD erfolgt ausschließlich auf schriftlichen Antrag. Das Gerät zum Beschreiben der Karten ist fest im Fahrzeug installiert und verschlossen. Ein Zugriff auf die Speicherkarten im Fahrzeug ist nur den Einsatzleitern der Wache mit einem speziellen Schlüssel möglich. Die Speicherkarten können an zentraler Stelle über ein spezielles Lesegerät, das an einem eigens dafür vorgesehenen Notebook angeschlossen ist, ausgelesen werden. Ein Auswählen von Bildsequenzen ist dabei nicht möglich. Die Aufzeichnung wird komplett übertragen und mit einer Signatur versehen, die nach Darstellung der Polizei Bremen beweissicher ist. Bei nachträglicher Veränderung von Videodaten wird die Signatur ungültig. Die Überprüfung dieser Signatur erfolgt mit einer speziell dafür vorgesehenen Software.

Da es sich hier um die automatisierte Verarbeitung personenbezogener Daten handelt, habe ich eine Verfahrensbeschreibung gefordert. Schwerpunktmäßig von Interesse ist aus technischer Sicht die Zugriffs- und Eingabekontrolle sowie das Verfahren zur Signierung der Videodaten, aus rechtlicher Sicht ist die „unverzügliche" Löschung klärungsbedürftig. Zudem ist die Zweckbindung der Aufzeichnungen („zur Verfolgung von Straftaten, die sich gegen Polizeivollzugsbeamte gerichtet haben") zu beachten. Die Aufzeichnungen dienen nicht dazu, (Verkehrs)Ordnungswidrigkeiten zu beweisen.

9.2 Videoüberwachung der „Discomeile“

Im Anschluss an die Vorfälle auf der sog. Discomeile Anfang des Jahres 2006 hat die Polizei Bremen ein Konzept zur Durchführung von Videoüberwachungsmaßnahmen nach § 29 Abs. 3, 4 Bremisches Polizeigesetz (BremPolG) erarbeitet. Im Juli 2006 erhielt ich die Angebote verschiedener Anbieter sowie den Vermerk einer Ortsbegehung zur Prüfung vorgelegt. In einem ersten Schreiben vom Juli 2006 wies ich darauf hin, dass vor der technischen Ausgestaltung der Maßnahme zunächst die Frage zu klären sei, ob überhaupt die gesetzlichen Voraussetzungen für eine Videoüberwachung vorliegen. Ich bat um weitere Informationen und wies auf einige ortsspezifische Einschränkungen hin (Schwärzen der Aufnahmebereiche von Privatwohnungen, unklare örtliche Reichweite, erhöhte Kriminalitätsbelastung an bestimmten Tagen und nur zu bestimmten Zeiten). Im Dezember 2006 stellte die Polizei Bremen mir ihr technisches Konzept vor und übersandte im Vorfeld den Entwurf einer Verfahrensbeschreibung. Einsatztaktisch wurde dabei eine 24-stündige Überwachung vorgesehen. Erneut wies ich auf die Betroffenheit von Grundrechten der Anwohner (Geschäfte und Privatwohnungen) hin und den ausstehenden Nachweis der erhöhten Kriminalitätsbelastung rund um die Uhr.

Ende Januar 2007 wurde mir der Entwurf der Deputationsvorlage zur stationären Videoüberwachung an der „Discomeile“ zugeleitet. In meiner Stellungnahme wies ich auf verschiedene technische Fragen hin, etwa zur Datenübertragung und Datensicherheit, die noch offen waren. Zudem enthielt die Deputationsvorlage vielfältige weitere Mängel, z. B. eine falsche Rechtsgrundlage und Zielsetzung und legte teilweise falsche tatsächliche Angaben zugrunde, die ich korrigierte. Auch ging die geplante Überwachung örtlich über die „Discomeile“ hinaus und sollte von 18.00 Uhr bis 10.00 Uhr am Folgetag andauern. Hier erreichte ich eine örtliche und zeitliche Einschränkung auf die „Discomeile“ und die Zeiten von 20.00 Uhr bis 8.00 Uhr am Folgetag, d. h. vor allem außerhalb der normalen Ladenöffnungszeiten.

Im November 2007, nachdem die Polizei Bremen etliche technische Probleme gelöst hatte, nahm ich erneut zu dem gewählten technischen Konzept Stellung und stellte konkrete Sicherheitsanforderungen. Auch wurde ich an der Ausgestaltung der Schilder und deren Standort beteiligt, die einen besonders wichtigen Aspekt für die Erkennbarkeit der Maßnahme und damit der Transparenz für die Betroffenen bedeuten. Am 21. Dezember 2007 begann die Videoüberwachung. Es ist geplant, ihren Einsatz im Jahr 2008 vor Ort bei der Polizei Bremen zu überprüfen.

9.3 Einsatzleitzentrale in Bremen

Im Dezember 2005 habe ich den Einsatz von Softwareprodukten bei der Einsatzleitzentrale der Polizei Bremen vor Ort angesehen. Das Produkt FELIS - „Flexibles Einsatzleitsystem Innere Sicherheit“ - wird eingesetzt zur Erfassung und Dokumentation von Notrufen. Dabei wird die von der Telefonanlage übermittelte Rufnummer bei Eingang eines Notrufs automatisch in die formulargestützte Notruferfassung aufgenommen. Der Bearbeiter ergänzt diese Daten und leitet sie an den Funksprecher zur Koordinierung der Einsätze weiter. Darüber hinaus werden die Gespräche der Einsatzleitzentrale aufgezeichnet und sollen für einen Zeitraum von drei Monaten gespeichert werden.

Eine Verfahrensbeschreibung, wie sie nach § 8 BremDSG erforderlich ist und die die getroffenen Sicherheitsmaßnahmen beschreibt, lag zu diesem Zeitpunkt nicht vor und wurde im Januar 2006 mit Übermittlung meines Berichts zur Ortsbesichtigung angefordert.

Die Ausfertigung und Übersendung der gesetzlich vorgeschriebenen Unterlagen wurde mit dem Hinweis auf technische Umstellungen verschoben. Nach mehreren Erinnerungen übersandte die Polizei Bremen mir ein Jahr später, Ende Januar 2007, eine erste Verfahrensbeschreibung. Ich nahm noch im gleichen Monat dazu Stellung. Die technischen und organisatorischen Maßnahmen wurden nicht vollständig und nur rudimentär beschrieben. Ich habe daher nochmals um ergänzende Angaben gebeten sowie nach dem Ergebnis der Vorabkontrolle, die durch den behördlichen Datenschutzbeauftragten durchgeführt werden muss.

Nachdem weitere zehn Monate vergangen waren und ich trotz wiederholter Erinnerungen und Rücksprachen keine weiteren Informationen erhalten habe, habe ich mich an den Polizeipräsidenten gewandt. Im Januar 2008 habe ich eine angepasste Verfahrensbeschreibung erhalten, die ich derzeit prüfe.

9.4 Automatische Kennzeichenerfassung

Der Polizeivollzugsdienst darf bei Kontrollen im öffentlichen Verkehrsraum durch den offenen Einsatz technischer Mittel zur elektronischen Erkennung von Kfz-Kennzeichen personenbezogene Daten zum Zwecke des sofortigen automatischen Abgleichs mit dem Fahndungsbestand erheben. Dies wurde durch Änderung des Bremischen Polizeigesetzes (BremPolG) vom 23. Februar 2006 (dort § 29 Abs. 6) möglich.

Durch Anfragen der Presse bin ich darauf aufmerksam gemacht worden, dass die Polizei Bremen Kennzeichenlesegeräte testet. Ich habe den behördlichen Datenschutzbeauftragten der Polizei Bremen um Mitteilung gebeten, in welchem Zeitraum die Testphase durchgeführt wird und habe einen kurzfristigen Prüftermin innerhalb der Testphase wahrgenommen. Die Polizei Bremen testete zwei verschiedene Geräte nebst Software. Die ersten Tests fanden im Rahmen von Verkehrskontrollen statt und waren bereits abgeschlossen. Für die Vergleiche der Kennzeichen der vorbeifahrenden Kraftfahrzeuge mit sogenannten Fahndungsnotierungen wurden Datenbestände des polizeilichen Informationssystems des BKA (INPOL) und Auszüge aus dem des Schengener Informationssystems (SIS) verwendet.

Das bei dem Prüftermin vorgeführte Fahrzeug war mit einer Videokamera ausgestattet, die mit einem mobilen Notebook verbunden wurde, auf dem die benannten Datenbestände gespeichert worden sind. Die Kamera lieferte Videobilder der vorbeifahrenden Fahrzeuge. Der Fahrer des vorbeifahrenden Fahrzeugs war dabei nicht erkennbar. Das Kennzeichen wurde mehrfach beim Heranfahren aus unterschiedlicher Entfernung (z. B. 50, 20, 10 Meter) von dem System gelesen (Erkennungssicherheit ca. 85 – 96 %). Die Software zeigte dabei in einem Windows-Fenster das gelesene Kennzeichen an. Die letzten elf Kennzeichen standen zur Ansicht in einem weiteren Windows-Fenster zur Verfügung. Ein Sichtvergleich der durch die Software gelesenen Kennzeichen mit dem tatsächlichen Fahrzeug ergab zu diesem Zeitpunkt keine Fehler.

In der getesteten Software gab es verschiedene Konfigurationsmöglichkeiten zur Bildspeicherung. Es konnte definiert werden, dass kein Bild gespeichert wird, dass alle Bilder gespeichert werden (z. B. im Rahmen einer Ringfahndung) oder dass nur die „Treffer“ gespeichert werden. Beim Test war die Einstellung „Treffer speichern“ eingestellt. Im Falle eines konkreten Einsatzes ist organisatorisch und technisch sicherzustellen, dass jeweils nur die für den Einsatz erforderliche Software aktiviert werden kann.

In diesen ersten Tests hat es Probleme beim Lesen der Kennzeichen gegeben, u. a. durch nicht reflektierende ausländische Kennzeichen (z. B. in Mittel- und Osteuropa keine Pflicht), durch Verschmutzung oder Beulen in Kennzeichen sowie durch schlechte Lichtverhältnisse.

Ich habe gegenüber der Polizei Bremen deutlich gemacht, dass bei Einsatz einer automatischen Kennzeichenüberwachung eine Verfahrensbeschreibung zu erstellen ist. Dabei sind insbesondere die technischen und organisatorischen Maßnahmen (z. B. Festplattenverschlüsselung, Kennwörter, sichere Aufbewahrung) zu benennen. Hier ist ein besonderer Schutz vorzusehen, da das Notebook den aktuellen INPOL- und Schengen-Fahndungsbestand und damit äußerst sensible Daten enthält.

Im Anschluss an die Demonstration der automatischen Kennzeichenüberwachung wurde vereinbart, dass die Polizei Bremen mich über den weiteren Verlauf der Tests und das Ergebnis informiert. Im

März 2007 teilte mir der behördliche Datenschutzbeauftragte der Polizei Bremen mit, dass eine Realisierung der Maßnahme aus Kostengründen derzeit nicht weiter verfolgt und die Angelegenheit zu einem späteren Zeitpunkt wieder aufgegriffen werde. Insoweit kann die verfassungsrechtliche Debatte über die Zulässigkeit dieses Instruments abgewartet werden.

9.5 Eingaben im Bereich der Polizeien des Landes Bremen

Auch im vergangenen Jahr erreichten mich wieder eine Vielzahl von Eingaben, die die Polizei betrafen. Wenige möchte ich exemplarisch darstellen. Verschiedentlich habe ich Betroffene bei der Ausübung ihres Rechts auf Auskunft, Berichtigung, Sperrung und Löschung ihrer bei der Polizei Bremen gespeicherten personenbezogenen Daten unterstützt. So erreichte ich die Löschung von Einträgen, beispielsweise weil sich aus dem Einstellungsbescheid der Staatsanwaltschaft ergab, dass bereits der Tatbestand des angezeigten Delikts nicht erfüllt war oder Betroffene, die Zeugen gewesen waren, versehentlich als Tatverdächtige aufgeführt wurden.

In einem Fall stellte ich bei meiner Prüfung fest, dass ein Petent aufgrund des Inhalts von vier Schreiben, die er an den Polizeipräsidenten gerichtet hatte, den personenbezogenen Hinweis „psychisch auffällig“ erhalten hatte. Die Polizei hatte eine solche Speicherung zunächst bestritten, da die Einstufung auf der Einschätzung eines Polizeibeamten beruhte und nicht eines Arztes, wie polizeiintern vorgesehen. Derartige Hinweise zur Eigensicherung der Beamten haben in der Praxis für das Verhalten der Polizeibeamten große Bedeutung. Fehler bei der Vergabe können daher schwerwiegende Konsequenzen nach sich ziehen. Es ist für den Betroffenen auch praktisch kaum möglich, den Hinweis berichtigen oder löschen zu lassen. Wie soll er nachweisen, dass er nicht „psychisch auffällig“ ist, wenn es keine belastbare ärztliche Beurteilung gibt? Die Polizei stimmte mir daher zu, dass der Hinweis zu löschen war. Zudem war der Petent im polizeilichen Informationssystem unter dem Datum seiner Schreiben jeweils als „Tatverdächtiger“ eines „sonstigen Delikts“ mit Deliktschlüssel vermerkt, obwohl kein Delikt begangen, keine Anzeige erstattet oder Ermittlungen aufgenommen worden waren. Auch fehlten Angaben zu den Umständen der Eintragung, so dass diese nicht nur unrichtig, sondern auch ungeeignet war, einem abrufenden Polizeibeamten Informationen für sein weiteres Vorgehen zu vermitteln. Ferner war der Deliktschlüssel auch noch in sich fehlerhaft und widersprüchlich vergeben worden. Nach dem Deliktschlüssel war der Petent bereits aufgrund einer gerichtlichen Verfügung nach dem Psychisch-Kranken-Gesetz (PsychKG) untergebracht worden, was aber nicht der Fall gewesen ist. Auch hier erreichte ich eine Korrektur. Schließlich teilte die Polizei mir auch noch mit, dass die Schreiben des Petenten, die zu den Eintragungen im polizeilichen Informationssystem geführt hatten, sich nicht mehr vollständig in der Akte befanden. Es ist der Polizei daher gar nicht mehr im Einzelnen möglich, den Hintergrund der Einträge nachzuvollziehen. Auch insoweit habe ich die Polizei aufgefordert, die Datenspeicherung zu korrigieren.

In einem anderen Fall rief mich ein Petent an und berichtete, dass ihn abends unter seiner Privatnummer eine fremde Frau angerufen habe und ihm sagte, er sei Halter eines bestimmten Fahrzeugmodells in einer bestimmten Farbe und seine Tochter habe heute morgen in seiner Wohnstraße ihren Sohn angefahren. Als der Petent wissen wollte, woher die Frau dies alles wisse, teilte sie mit, sie sei die Frau eines Polizeibeamten. Im Laufe des Abends meldete sich dann der Beamte und erklärte die Angelegenheit für erledigt. Der Petent hatte zu diesem Zeitpunkt bereits einen Mann mit seinem Sohn in der Wohnstraße gesehen, der die Wagen der Nachbarn untersuchte. Es stellte sich heraus, dass der Sohn eines Polizeibeamten morgens von einem Fahrzeug angefahren worden war und vom Fahrrad gestürzt war. Die junge Fahrerin hatte den Sohn im Wagen zur Schule gebracht und erwähnt, dass sie „gleich hier“ wohne. Der Vater und Polizeibeamte hatte daraufhin von seiner dienstlichen Möglichkeit einer Kfz-Halterabfrage und Melderegisterabfrage Gebrauch gemacht

und mögliche Halter des Fahrzeugtyps in der Gegend und deren Familienverhältnisse (Tochter in bestimmten Alter) ermittelt, „zwecks Geltendmachung schadensersatzrechtlicher Ansprüche“. Allerdings war der angerufene Petent bzw. seine Tochter nicht der vermeintliche Unfallbeteiligte. Seine Tochter lebte samt Fahrzeug in einem anderen Bundesland. Der Beamte hatte daraufhin mit seinem Sohn die Umgebung des Unfallortes erneut abgesucht und das Verursacherfahrzeug ausfindig gemacht. Erneut tätigte der Beamte eine Kfz-Halterabfrage und Melderegisterabfrage und suchte die Telefonnummer aus dem Telefonbuch. Auch diese Familie rief er zur „Schadensregulierung“ an. Eine Strafanzeige wegen Unfallflucht oder fahrlässiger Körperverletzung fertigte der Beamte nicht.

Ich teilte der Polizei Bremen mit, dass das Vorgehen des Beamten in mehrfacher Hinsicht datenschutzwidrig sei, eine Ordnungswidrigkeit darstelle und zudem auch aus polizeitaktischer Sicht fragwürdig sei. Die Polizei führte daraufhin ein ausführliches Gespräch mit dem Beamten über seine datenschutzrechtlichen Pflichten. Der Beamte unterzeichnete eine Datenschutzerklärung. Zugleich erkundigte ich mich, ob es bei der Polizei Bremen Regelungen gibt, die eine Ermittlung von Beamten einschränkt, sofern eigene Belange betroffen sind. Andernfalls sei es nicht möglich, zwischen Abfragen zu dienstlichen bzw. privaten Zwecken zu unterscheiden. Die Polizei teilte mir daraufhin mit, dass derartige Regelungen nicht bestünden und beharrte darauf, dass mangels Wiederholungsgefahr weiterreichende Maßnahmen nicht erforderlich seien. Dies halte ich im Ergebnis für unbefriedigend und plane, mich für eine derartige Regelung einzusetzen.

In einem weiteren Fall hatte sich ein Petent an mich gewandt, der eine zivilrechtliche Streitigkeit über die Abwicklung von Werkstattkosten austrug, die auch in einer Strafanzeige wegen Betrugs gegen ihn mündete. Dabei war er von dem Werkstattbesitzer im Beisein seines Vaters, der Polizeibeamter ist, unter Druck gesetzt und ihm waren Schwierigkeiten angedroht worden. Wenige Zeit später erhielt der Arbeitgeber des Petenten ein anonymes Schreiben, in dem offengelegt wurde, dass er strafrechtlich in Erscheinung getreten war. Aufgrund des zeitlichen und inhaltlichen Zusammenhangs überprüfte ich die Protokolle der Zugriffe im polizeilichen Informationssystem auf die Daten des Petenten und stellte fest, dass der Vater des Werkstattbesitzers zunächst ohne erkennbaren dienstlichen Hintergrund auf die Daten zugegriffen hatte. Die Ermittlungen der Polizei führten zu einem Strafverfahren wegen des Verrats von Dienstgeheimnissen, das im Ergebnis jedoch eingestellt wurde, da nicht gerichtsfest nachweisbar war, dass die durch den Zugriff erlangten Informationen von dem Beamten weitergegeben worden waren oder er Urheber des anonymen Drohbriefes ist. Die Staatsanwaltschaft räumte allerdings ein, dass es sich insoweit um eine wirklichkeitsnahe Vermutung handele. Erschwert wurde das Verfahren dadurch, dass der Petent um jeden Preis vermeiden wollte, dass sein Arbeitgeber als Zeuge Näheres zu dem Drohbrief aussagt, weil er dann mit einem Verlust seines Arbeitsplatzes rechnete. Ich forderte die Polizei nach Einstellung des Strafverfahrens auf, zumindest den unberechtigten Zugriff disziplinarisch zu ahnden, da der Beamte als Begründung für den Zugriff angab, er habe überprüfen wollen, ob sein Sohn ihn bei der Strafanzeige wegen Betrugs als Zeugen angegeben habe. Insoweit handelte der Beamte jedoch aus privaten Gründen. Andere Privatpersonen könnten eine derartige Abfrage im polizeilichen Informationssystem nicht veranlassen. Auch ist die Aussage lebensfremd, da der Beamte nur seinen Sohn hätte fragen müssen und über die Abfrage eine Vielzahl weiterer Informationen erhielt. Ich bat daher um Stellungnahme, weshalb die Polizei Bremen keinen Raum für Maßnahmen sieht, den Verstoß angemessen zu ahnden. Ich wies auch darauf hin, dass das Fehlen einer Regelung zum Tätigwerden von Beamten bei eigener Betroffenheit die Beurteilung der Zugriffe erschwert. Eine Antwort der Polizei Bremen steht bislang aus.

9.6 Prüfung der Antiterrordatei beim LKA und Landesamt für Verfassungsschutz

Auf Grundlage des Antiterrordateiengesetzes vom 22. Dezember 2006 sollte bis März 2007 bei den beteiligten Behörden, u. a. dem Landeskriminalamt (LKA) Bremen und dem Landesamt für Verfassungsschutz Bremen, die Infrastruktur für den Betrieb der Antiterrordatei aufgebaut und die Datei in den Wirkbetrieb genommen werden.

Ich habe daher im Mai und Juni 2006 die Antiterrordatei bei den beteiligten Behörden in Bremen geprüft und mich u. a. über die vorgenommenen technischen und organisatorischen Maßnahmen, z. B. Verschlüsselungen oder Zugriffsberechtigungen, informiert. Dabei musste ich feststellen, dass die Infrastruktur vorhanden und die Antiterrordatei einsatzbereit war, jedoch das Befüllen der Datei noch andauerte. Dies lag nicht unbedingt an einer großen Zahl von Einträgen, sondern war der Personalknappheit bei Polizei und Verfassungsschutz und der Sicherstellung der Qualität der Daten geschuldet. Die meisten Probleme, die das Gesetz aufwirft (vgl. 30 JB, Ziff. 9.8) waren in der Praxis in Bremen daher noch nicht relevant geworden. Einzelne Fragen habe ich in einem vorläufigem Prüfbericht festgehalten und beabsichtige im Jahr 2008, wenn die Befüllung voraussichtlich abgeschlossen ist, die Prüfung fortzusetzen.

9.7 Eingaben im Bereich des Verfassungsschutzes

Auch in diesem Jahr haben sich wieder verschiedene Petenten mit Eingaben bzgl. des Landesamtes für Verfassungsschutz (LfV) an mich gewandt. Oftmals werde ich eingeschaltet, wenn die Betroffenen Einsicht in ihre beim Landesamt für Verfassungsschutz gespeicherten personenbezogenen Daten nehmen möchten oder wissen möchten, ob sie Gegenstand einer nachrichtendienstlichen Maßnahme sind. Regelmäßig richtet sich die Anfrage sowohl an die Polizei Bremen als auch das LfV. Das Landesamt kann insoweit die Auskunft in bestimmten Fällen verweigern, muss die Betroffenen jedoch darauf hinweisen, dass sie mich anrufen können. Mir wird dann vom Landesamt Einsicht gewährt bzw. Auskunft erteilt. Allerdings kann ich den Petenten diese vertraulichen Informationen nicht mitteilen, sondern lediglich die Rechtmäßigkeit bzw. Unrechtmäßigkeit der Datenverarbeitung prüfen und das Ergebnis festhalten. Daneben bin ich z. B. in einem Einbürgerungsverfahren angerufen worden, in dem dem Betroffenen die Einbürgerung aufgrund nachrichtendienstlicher Erkenntnisse verwehrt, die Erkenntnisse selbst aus Gründen des Quellenschutzes jedoch nicht mitgeteilt wurden. Auch hier konnte ich durch eine Einsichtnahme die Rechtmäßigkeit der Datenverarbeitung sicherstellen. Zum Prüfumfang zählt dabei selbstverständlich auch, ob die Weigerung der Behörde zur Auskunftserteilung rechtmäßig ist.

9.8 Verfassungsbeschwerdeverfahren gegen das Antiterrordateiengesetz

Im Juli 2007 erhielt ich vom Bundesverfassungsgericht den Abdruck der Verfassungsbeschwerde zum Antiterrordateiengesetz (1 BvR 1215/07) mit der Bitte, zu den aufgeworfenen verfassungsrechtlichen Fragen eine Stellungnahme abzugeben. Die Datenschutzbeauftragten des Bundes und der Länder einigten sich, eine gemeinsame Stellungnahme zu formulieren. Die Vorarbeiten hierfür übernahm der Arbeitskreis Sicherheit der Datenschutzkonferenz und dort vor allem die Länder Schleswig-Holstein und Berlin.

In ihrer gemeinsamen Stellungnahme vertreten die Datenschutzbeauftragten, dass das Antiterrordateiengesetz (ATDG) einen nicht gerechtfertigten Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt, da es gegen die Grundsätze der Normenklarheit, Bestimmtheit und der Verhältnismäßigkeit verstößt. Dies betrifft die Beschreibung des betroffenen Personenkreises und den Umfang der zu speichernden Daten, aber auch die unklaren Zugriffs- und Verwendungsregelungen sowie die unzureichenden Löschungsregelungen und Auskunftsrechte der Betroffenen. Aufgeworfen wird auch die Frage, inwieweit das ATDG dem Gebot, Polizeibehörden und Nachrichtendienste zu trennen, genügt.

9.9 Entscheidung des Bundesverfassungsgerichts zur Videoüberwachung

Das Bundesverfassungsgericht hat mit Beschluss vom 23. Februar 2007 (1 BvR 2368/06) entschieden, dass eine Videoüberwachung öffentlicher Plätze in Regensburg nicht auf die allgemeinen Übermittlungsvorschriften des Bayerischen Landesdatenschutzgesetzes gestützt werden kann. Es fehle dabei an einer hinreichend bestimmten und normenklaren Rechtsgrundlage, um den durch die Videoüberwachung verursachten Eingriff in das Grundrecht auf informationelle Selbstbestimmung zu rechtfertigen. Das Urteil enthält einige grundlegende allgemeine Ausführungen zur Videoüberwachung. Das Bundesverfassungsgericht betont in der Entscheidung, dass eine Videoüberwachungsmaßnahme einen Eingriff von erheblichem Gewicht darstellt, weil er verdachtslos und mit großer Streubreite zahlreiche Personen betrifft, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben. Zudem dient die Videoüberwachungsmaßnahme dazu, belastende hoheitliche Maßnahmen vorzubereiten und das Verhalten der den Raum nutzenden Personen zu lenken. Das infolge der Aufzeichnung gewonnene Bildmaterial kann in vielfältiger Weise ausgewertet, bearbeitet und mit anderen Informationen verknüpft werden.

9.10 Entwurf eines Bundesmeldegesetzes

Im Zuge der Föderalismusreform wurde das Meldewesen in die ausschließliche Gesetzgebungskompetenz des Bundes überführt. In Ergänzung der bisherigen kommunalen Register plant das Bundesministerium des Innern den Aufbau eines Bundesmelderegisters (BMR). Ich habe den Senator für Inneres und Sport sowie den Magistrat der Stadt Bremerhaven und das Stadtamt Bremen gebeten, u. a. folgende grundsätzlichen Positionen bei einer anstehenden Gesetzesberatung zu vertreten:

Eine Reform des Melderechts muss den Umfang der im Meldewesen gespeicherten Daten einer kritischen Prüfung unter den Gesichtspunkten der Erforderlichkeit und der Zweckbindung unterziehen.

Ein zentrales Bundesmelderegister und die damit verbundene mehrfache Datenhaltung bei Bund und Länder ist nicht erforderlich. Die Modernisierung des Meldewesens kann durch eine Vernetzung der vorhandenen Melderegister erreicht werden. Hierfür hat man bereits 2002 auf Drängen des Bundes den Datenaustausch im Meldewesen und damit die Voraussetzungen für einen effizienten und sicheren Datenaustausch geschaffen.

Der vollständige Meldedatenbestand muss bei den jeweiligen kommunalen Meldeämtern und unter deren Verantwortung verbleiben.

9.11 Mobiler Bürgerservice

Das Stadtamt Bremen will das Angebot von Verwaltungsdienstleistungen durch Nutzung neuer technischer Entwicklungen der Datenübertragung weiter entwickeln und modernisieren. Im Oktober 2006 wurde ich darüber informiert. Das Pilotprojekt trägt den Namen ”Mobiler Bürgerservice“.

Es war geplant, durch Einsatz mobiler Endgeräte ein Angebot an wechselnden Standorten in verschiedenen Stadtteilen Bremens anzubieten. Dabei sollte es sich um Anlaufstationen handeln wie beispielsweise Einkaufszentren, Stadtbibliotheken oder Senioreneinrichtungen, die vor allem für Bürger mit Bewegungseinschränkungen gut erreichbar sein sollten. Begonnen werden sollte mit dem am stärksten nachgefragten Angebot, dem Meldewesen.

Ich habe von der ersten Projektsitzung an darauf aufmerksam gemacht, dass ein Datenschutzkonzept für den Anwendungsfall „Mobiler Bürgerservice“ erstellt werden muss, da bereits in dem Pilotprojekt personenbezogene Originaldaten verarbeitet werden.

Da für die Anbindung der Standorte an das Stadtamt die bestehende bremische Infrastruktur genutzt werden sollte, war eine Betrachtung dieser Infrastruktur unter den zuvor genannten Anforderungen nach § 7 BremDSG für das Projekt „Mobiler Bürgerservice“ und das zu erstellende Datenschutzkonzept notwendig.

Das Projekt „Mobiler Bürgerservice“ wurde in zwei Phasen geteilt. In der ersten Phase wählte die Arbeitsgruppe Standorte aus, die über eine Datenleitung zur Nutzung des BVN verfügten, und zwar die Stadtbibliothek Bremen und das Ortsamt Osterholz. Das Stadtamt legte dafür im Dezember 2006 ein entsprechendes Datenschutzkonzept vor. Meine Stellungnahme erhielt das Stadtamt Bremen im Februar 2007. Es ergaben sich u. a. Fragen zur Anbindung der genannten Standorte an das Stadtamt Bremen, zur Leitungsverschlüsselung, zur Härtung der Arbeitsplätze und Protokollierung der Zugriffe.

Im Februar 2007 wurde ich über den Beginn der zweiten Phase dieses Projektes informiert, in dem mobile Endgeräte eingesetzt werden sollten. Aufgrund der vorgesehenen Funkverbindung wurde es möglich, Senioreneinrichtungen und Einkaufszentren als neue Standorte einzubeziehen. Das Stadtamt sicherte mir eine Ende-zu-Ende-Verschlüsselung vom eingesetzten Endgerät bis zur Anwendung im Stadtamt sowie einen zertifizierten Zugang über ein Security-Gateway zu. Des Weiteren habe ich Vorgaben zur eingesetzten Hardware gemacht, wie z. B. den Einsatz einer Firewall, eine Festplattenverschlüsselung und lokale Sicherheitssoftware. Außerdem forderte ich die klare Definition der Administrationsverantwortung.

Im April des Berichtsjahres habe ich mir den für dieses Projekt angefertigten „Bürgeramtkoffer“ angesehen. In diesem sind neben einem Notebook eine so genannte Desktop-Box mit zentralem Stromanschluss und USB-Hub sowie ein Drucker und ein Scanner untergebracht. Die Festplatte des Notebooks ist verschlüsselt. Die Einwahl über das Security-Gateway wurde demonstriert, jedoch konnten bei diesem Termin keine detaillierten Angaben zum eingesetzten Zertifikat sowie zum Aufbau des verschlüsselten Tunnels gemacht werden. Die dazu vorgelegte Skizze war unvollständig und sollte noch ergänzt werden. Eine abschließende Bewertung ist mir erst nach Vorlage des vollständigen Datenschutzkonzepts möglich. Dieses sollte auch organisatorische Regelungen (z. B. Ablaufplan für Mitarbeiter) sowie Konzepte für Wartung und Updates, zur Administration und Angaben

zur Protokollierung enthalten. Auch die noch offenen Punkte zum Rahmendatenschutzkonzept sollten darin Berücksichtigung finden.

Im Juli diesen Jahres wies ich erneut auf die noch ausstehenden Unterlagen zum Projekt „Mobiler Bürgerservice“ hin und erhielt im August einen Abschlussbericht. Ich bemängelte nochmals, dass eine Anpassung des Datenschutzkonzepts für die erste Phase nicht erfolgt war und dass ich für die zweite Phase kein Datenschutzkonzept erhalten hatte. Eine Fortführung bzw. Ausdehnung des Projektes auf weitere Standorte kann nur erfolgen, wenn bis dahin ein vollständiges Datenschutz- und IT-Sicherheitskonzept vorliegt.

Im Dezember 2007 hat mich das Stadtamt informiert, das Projekt „Mobiler Bürgerservice“ werde aufgrund mangelnder personeller Ressourcen derzeit nicht fortgeführt.

9.12 Online-Anmeldung von Kraftfahrzeugen durch Autohäuser

Um die Zulassung von Kraftfahrzeugen zu beschleunigen, können autorisierte Zulassungsdienste und Autohäuser die Kfz- und Halterdaten via Internet im Rahmen einer E-Government-Anwendung an die Zulassungsstellen übermitteln. Durch einen Link auf den Webseiten von Bremen.de gelangen sie auf die Seiten der Kfz-Zulassungsstellen des Stadtamtes Bremen. Im vergangenen Jahr hatte ich berichtet, dass die Daten ungeschützt übertragen wurden (vgl. 29. JB, Ziff. 9.2.3). Das Stadtamt hatte zugesagt, dies zu unterlassen und die Übertragung abzusichern. Geplant war die Umsetzung der Datenübertragung mittels des OSCI-Protokolls. Da es sich nicht um eine unmittelbare Zulassung von Fahrzeugen handelt, sondern nur um die vorbereitende Datenerfassung und die Übermittlung an die Zulassungsstellen, nahm das Stadtamt von einem Authentizitätsnachweis per elektronischer Signatur, wie es der zunächst geplante OSCI-Einsatz ermöglicht hätte, Abstand. Das Stadtamt teilte mit, durch den Geschäftsablauf bedingt würde die Identität des zukünftigen Halters und der Vertretungsvollmacht bei der Abholung der Dokumente geprüft. Das Verfahren sei so geändert worden, dass die Übermittlung der Daten für die Zulassung und die Anmeldung der Nutzer nunmehr verschlüsselt erfolge. Damit ist auf dem Transportweg ein angemessenes Datenschutzniveau erreicht.

9.13 Fingerabdruckdaten in Reisepässen

In Umsetzung der Verordnung (EG) 2252/2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten der Europäischen Union ausgestellten Pässen und Reisedokumenten hat Deutschland in einer ersten Stufe zum 1. November 2005 den biometrischen Reisepass eingeführt und in einem sog. RFID-Chip das Gesichtsbild elektronisch gespeichert. Ab 1. November 2007 kam die Speicherung von zwei Fingerabdrücken hinzu. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte sich bereits im Juni 2005 mit einer Entschließung dagegen gewandt und darauf hingewiesen, dass die Einführung biometrischer Reisepässe nicht automatisch zu mehr Sicherheit führt (vgl. 28 JB, Ziff. 19.11).

Vor der flächendeckenden Einführung sollte das Verfahren unter realen Bedingungen in ausgewählten Passbehörden getestet werden. Zu diesen gehörte die Passbehörde Bremerhaven. Im Dezember 2006 wurde ich um Stellungnahme zu dem bremischen Landesgesetz gebeten, mit dem die Teilnahme der Passbehörde Bremerhaven an der Testphase umgesetzt wurde. Ich habe eine Stellungnahme abgegeben, in der ich verschiedene Anforderungen aufgestellt habe, so z. B. zu rechtstechnischen Vorgaben, insbesondere der Veröffentlichung und Beachtung der Technischen Richtlinie für das Testverfahren durch das Bundesamt für Sicherheit in der Informationstechnik, wie zur Aufklärung der Bürger über die Teilnahmebedingungen.

Ende Mai 2007 habe ich vor Beendigung der Testphase der Passbehörde Bremerhaven einen Besuch abgestattet und mich vor Ort informiert. Zu diesem Zeitpunkt hatten etwa 400 Bürgerinnen und Bürger sich an 32 Geräten an zwei Standorten Reisepässe erstellen lassen. Probleme bei der Durchführung hatte es nicht gegeben. Die Passbehörde hatte ein vom Bundesministerium des Innern zur Verfügung gestelltes Informationsblatt für Bürger bereitgestellt und behördenintern eine Anweisung zur Durchführung des Feldtests erlassen. Beim Einscannen wurden erst von der einen, dann der anderen Hand der Zeigefinger eingescannt, wobei drei Bilder aufgenommen und das beste schließlich weiterverwendet wird. Ich stellte dabei fest, dass das System nicht erkennt, wenn der Zeigefinger der einen Hand bei einer der Aufnahme mit dem Zeigefinger der anderen Hand vertauscht wurde. Das System wählt dann u. U. einen falschen Fingerabdruck als den besten aus. Ich stellte ferner fest, dass die Fingerabdruckdaten entgegen § 23 a Abs. 3 Satz 7 PassG nicht getrennt von anderen Dateien mit Passantragsdaten gespeichert wurden. Die Übermittlung vom Arbeitsplatzrechner an den „Kommunikations-Server“ für die Übermittlung an die Bundesdruckerei erfolgte unverschlüsselt innerhalb des unsicheren (vgl. 23. JB, Ziff. 3.2) Magistrats-Netzes. Eine Änderung des Datenschutzkonzeptes mit Blick auf die Testphase war nicht erfolgt.

Nach der Aufnahme des Produktionsbetriebes bei der Beantragung eines ePasses im November 2007 ist im Jahr 2008 ein erneuter Besuch bei der Passbehörde geplant, bei dem ich u. a. die oben genannten Punkte erneut aufgreifen werde.

9.14 Anmeldung zur Eheschließung im Internet (xStA-Bürger)

Im Sommer 2006 wurde ich durch einen Presseartikel auf ein bei den Standesämtern eingeführtes Datenverarbeitungsverfahren „xStA-Bürger“ aufmerksam. Danach können heiratswillige Bürgerinnen und Bürger sich einen Weg zum Standesamt ersparen, indem sie durch Eingabe verschiedener Daten zu ihrer Person, etwaigen Kindern, ihren Eltern und Trauzeugen, die Anmeldung zur Eheschließung beschleunigen. Das Verfahren wird nicht direkt beim Stadtamt Bremen, sondern im Wege der Auftragsdatenverarbeitung durch das anbietende Unternehmen von einem Rechner in Frankfurt aus betrieben.

Im Sommer 2006 wandte ich mich zunächst an die Standesämter Bremen-Mitte und Bremen-Nord und bat um die Übersendung der Verfahrensbeschreibung und des Datenschutzkonzeptes einschließlich der Unterlagen zur Auftragsdatenverarbeitung. Im November 2006 wurde mir vom Stadtamt Bremen mitgeteilt, dass meine Auffassung zum Bestehen eines Auftragsdatenverarbeitungsverhältnisses geteilt werde, allerdings keine Unterlagen vorhanden seien. Diese sollten erstellt werden. Im Sommer 2007 habe ich mich nach dem Stand der Erarbeitung erkundigt, da weiterhin die gesetzlich vorgeschriebene Dokumentation des Verfahrens und der getroffenen technisch-organisatorischen Maßnahmen ausstand, um das Verfahren datenschutzrechtlich angemessen zu prüfen. Vom behördlichen Datenschutzbeauftragten des Stadtamtes Bremen wurde mir mitgeteilt, dass ihm mittlerweile Entwürfe zur Verfahrensbeschreibung und zum Datenschutzkonzept nebst Anlagen vorlägen, aber weiterer Gesprächsbedarf mit den Erstellern bestünde. Seitdem warte ich weiter auf die angekündigte Übersendung der Unterlagen.

9.15 BVerfG zur TK-Überwachung im Fall Masri

Mit Beschluss vom 30. April 2007 (2 BvR 2151/06) entschied das Bundesverfassungsgericht, dass die Überwachung des Telefon- und Telefaxanschlusses der Rechtsanwaltskanzlei, die den mutmaßlich von Geheimdienstkreisen entführten Khaled El Masri vertrat, eine Verletzung des Fernmeldegeheimnisses und der Berufsausübungsfreiheit des Beschwerdeführers darstellt.

Das Verfassungsgericht ließ dabei die Begründung des anordnenden Gerichts nicht gelten, aufgrund der Medienberichterstattung eineinhalb Jahre nach der Entführung müsse damit gerechnet werden, die Entführer träten mit der Kanzlei in Verbindung. Hierbei handele es sich lediglich um Vermutungen. Das Verfassungsgericht hat damit die hohen Anforderungen an die Rechtfertigung von Eingriffen in das Fernmeldegeheimnisses hervorgehoben und einer allzu ausufernden Praxis bei der Telekommunikationsüberwachung entgegengewirkt.

9.16 Verfahren ADVIS und BONITAET beim Stadtamt Bremen

Im Juli 2007 übersandte mir das Stadtamt Bremen die Verfahrensbeschreibung und das Datenschutzkonzept für die Verfahren „AusländerDatenVerwaltungs- und InformationsSystem“ (ADVIS) und BONITAET, welches ein Programm zum Verwalten und Auswerten von Verpflichtungserklärungen ist, mit denen sich eine Person verpflichtet, für die Lebenskosten eines Ausländers im Bundesgebiet aufzukommen.

Im Juli 2007 übersandte ich dem Stadtamt Bremen meine Stellungnahme zu der Verfahrensbeschreibung und zum Datenschutzkonzept des Verfahrens BONITAET. Die Rechtsgrundlagen waren nicht zutreffend aufgeführt und die Darstellung der verarbeiteten Datenkategorien war teilweise zu allgemein oder unzutreffend. Aus technischer Sicht fehlte eine Authentifizierung und Protokollierung, so dass nicht nachvollzogen werden konnte, wer Eingaben oder Zugriffe in dem Programm tätigt. Das Stadtamt Bremen hat mir daraufhin im November 2007 verschiedene Änderungen mitgeteilt; offen blieb jedoch, wie viele Personen auf das Programm zugreifen, ob eine Anmeldung an dem Verfahren erfolgt und ob eine Protokollierung der Benutzeraktivitäten erfolgt. Daher habe ich Anfang Dezember 2007 einige ergänzende Informationen angefordert. Eine Antwort hierauf steht bislang aus.

Zu dem Verfahren ADVIS, dass deutlich umfangreicher ist als BONITAET, nahm ich im Dezember 2007 gegenüber dem Stadtamt Bremen Stellung. Dabei stellte ich fest, dass vor allem eine klare Trennung der Datenverarbeitung nach dem Aufenthaltsgesetz und der Aufenthaltsverordnung einerseits und dem Ausländerzentralregistergesetz und seiner Durchführungsverordnung fehlt. So kam es bei der Angabe der Rechtsgrundlagen, der Beschreibung der Datenkategorien und der Verwendungszwecke zu Unklarheiten und Unrichtigkeiten. Es wurden unzutreffende Rechtsgrundlagen genannt und zutreffende Rechtsgrundlagen weggelassen, die beschriebenen Daten entsprachen nicht den Rechtsgrundlagen und die Verwendungszwecke waren nicht vollständig genannt. Es wurden Fragen zum Trennungsgebot aufgeworfen, da unter ADVIS verschiedene Dateien geführt werden, für die ich zum Teil keine Rechtsgrundlage erkennen konnte. Die Darstellung der Löschfristen und Empfänger von Datenübermittlungen waren teilweise unvollständig oder unzutreffend. Daneben ergaben sich verschiedene Fragen zur Datensicherheit des Verfahrens, etwa zum Trennungsgebot, zur Weitergabe-, Zugriffs- und Verfügbarkeitskontrolle.

9.17 Übermittlung von Meldedaten an politische Parteien vor den Wahlen

Auch im Vorfeld der Wahlen zur Bremischen Bürgerschaft und zur Stadtverordnetenversammlung Bremerhaven wurden wieder von den Meldebehörden in Bremen und Bremerhaven Daten von wahlberechtigten Einwohnern an Parteien weitergegeben, die an der Wahl teilnehmen.

Die Meldebehörde Bremen übermittelte aus dem Einwohnermelderegister Dateien mit Einwohnerlisten an die CDU, die DVU und die Republikaner (REP). Aus dem Melderegister der Stadt Bremerhaven erhielten vor der Bürgerschafts- und der Stadtverordnetenwahl die CDU, die DVU und die Wählervereinigung „Bürger in Wut“ (BiW) Daten von Wahlberechtigten. Maßgeblich für den Umfang, der von der jeweiligen Datenübermittlung Betroffenen, ist dabei stets die Zugehörigkeit zu einer bestimmten Lebensaltersgruppe. Daten von Einwohnern, die nach § 33 Abs. 1 Meldegesetz (BremMeldG) gegen die Übermittlung ihrer Daten bei der Meldebehörde Widerspruch eingelegt hatten, wurden nicht übermittelt.

Schwerwiegende Mängel wurden bei der Überprüfung der Datenübermittlungen im Vergleich zu vorhergehenden Wahlen nicht festgestellt. Im Hinblick auf die öffentliche Bekanntmachung des Widerspruchs nach § 33 Abs. 1 Satz 7 BremMeldG war in Bremerhaven allerdings festzustellen, dass diese dort erst verspätet erfolgte. Ich habe die Meldebehörde Bremerhaven aufgefordert, bei künftigen Wahlen die sich aus § 33 Abs. 1 Satz 7 BremMeldG ergebende Frist zur Bekanntgabe von acht Monaten vor der jeweiligen Wahl einzuhalten.

9.18 Eingaben in Bezug auf politische Parteien und Wahlinitiativen im Zusammenhang mit den Wahlen

Im Vorfeld der Wahlen zur Bremischen Bürgerschaft und zur Bremerhavener Stadtverordnetenversammlung erhielt ich im Frühjahr des Berichtsjahrs mehrere Eingaben von Bürgern, die die Verarbeitung von Wählerdaten durch an der Wahl teilnehmende Parteien betrafen.

Eine Bürgerin beklagte sich dabei, dass sie von einer bestimmten Partei wiederholt Wahlwerbebriefe erhalten hatte, ohne dass sie hiermit einverstanden gewesen sei. Bereits den ersten Brief, den sie erhalten hatte, habe sie an die Partei zurückgeschickt mit der Aufforderung, ihr keine weitere Wahlwerbung zuzuschicken und ihre Daten zu löschen. Nach § 28 Abs. 4 BDSG hat der Betroffene das Recht, der Nutzung seiner Daten für Zwecke der Werbung zu widersprechen. Im Widerspruchsfall dürfen die gespeicherten Daten für Zwecke der Werbung nicht mehr genutzt werden. Diese Regelung gilt auch für Werbung zu politischen Zwecken. Erst auf meine ausdrückliche und wiederholte Aufforderung hin erklärte sich die Partei schließlich zum Verzicht auf weitere Wahlwerbung und die Löschung der Daten meiner Petentin bereit.

Auch aufgrund vorhergehender Presseartikel erhielt ich eine Vielzahl von Eingaben, die die telefonische Wahlwerbung einer Wahlinitiative betrafen. Bei Annahme des Anrufs erfolgte eine automatische Bandansage durch eine Privatperson, die zugleich der Spitzenkandidat der Wahlinitiative war und mit dieser im Wahlkampf verbunden wurde. Die Privatperson berichtete über einen von ihr gegründeten Verein, der Deutsche in Not unterstütze und endete mit der Bitte, die Person unter der im Telefonbuch angegeben Nummer anzurufen, wenn man Menschen kenne, die Hilfe benötigen. Unmittelbar vor der Wahl erfolgten weitere „freundliche Erinnerungsanrufe“. Daneben beschwerten sich verschiedentlich Betroffene, die Telefaxe der Privatperson bzw. des von ihr gegründeten Vereins erhalten hatten. Die Betroffenen beklagten sich darüber, dass sie in die Kontaktaufnahme per Telefon und Telefax nicht eingewilligt hätten. Ich habe die Wahlinitiative angeschrieben und meine Bedenken an der Zulässigkeit der telefonischen Wahlwerbung geäußert. Nach der Rechtsprechung verletzen unerbetene Telefonanrufe das Persönlichkeitsrecht der Betroffenen auch dann, wenn sie von einer politischen Partei während des Wahlkampfes erfolgen. Ihr Interesse, möglichst viele Stimmberechtigte für ihre Ziele zu gewinnen, muss hinter das Recht des Einzelnen auf Respektierung seines häuslichen Lebensbereiches zurücktreten. Zur näheren Aufklärung des Sachverhalts bat ich zunächst um die Beantwortung verschiedener Fragen, da insbesondere die Frage der Urheberschaft nicht klar war und offenbar auch bewusst so gehalten werden sollte.

Der Spitzenkandidat der Wahlinitiative bestritt, dass diese zu irgendeinem Zeitpunkt telefonische Wahlwerbung betrieben habe und drohte gerichtliche Schritte an. Nähere Auskunft zu den Telefonanrufen und Telefaxen, die ihm als Autor der automatischen Bandansage und Gründer des Vereins möglich gewesen wären, gab er nicht.

Da ich eine Verantwortlichkeit des Vereins, der sich in der automatischen Bandansage und über den Briefkopf der Telefaxe als Urheber zu erkennen geben sucht, nicht ausschließen konnte, habe ich mich Anfang Mai an den Hamburgischen Datenschutzbeauftragten zur Aufklärung des Sachverhaltes gewandt, da der Verein seinen Sitz in Hamburg hatte.

Der Hamburgische Datenschutzbeauftragte sah letztlich keinen Grund für sein Tätigwerden, da aller Voraussicht nach die Telefonnummern für die Anrufe und Telefaxe automatisiert ausgewählt und angerufen werden, ohne personenbezogenen Daten der Betroffenen zu speichern. Auch wurde der Aufwand einer kurzfristigen Prüfung als zu groß angesehen.

Dies habe ich im Ergebnis akzeptiert, da wenige Tage später die Bürgerschaftswahl stattfand und die Anrufe der Privatperson bzw. des Verein erwartungsgemäß endeten.

9.19 Neufassung der KpS-Richtlinien

In meinem 28. Jahresbericht (vgl. Ziff. 9.7) hatte ich gefordert, die Richtlinien über die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien) aus dem Jahr 1981 zu aktualisieren. Im Jahr 2006 wurde daraufhin ein erster Entwurf erstellt, der sich allerdings nur mit einem Teilbereich beschäftigte. Ende 2006 sagte der Senator für Inneres und Sport zu, den Entwurf bis zum Sommer 2007 abschließend zu überarbeiten.

Im Februar 2007 übersandte mir der Senator für Inneres und Sport eine überarbeitete Fassung, zu der ich Mitte Juni Stellung nahm und nach Vorlage einer aktualisierten Fassung erneut Ende Juli 2007. Mitte September 2007 wurde mir abermals ein Entwurf zur Stellungnahme übersandt, zu dem ich abschließend im Dezember 2007 Stellung bezog.

Inhaltlich habe ich neben einer Reihe von redaktionellen Änderungen und Aktualisierungen vor allem eine Einschränkung bei der Speicherung von personenbezogenen Daten von Kindern unter sieben Jahren und zwischen sieben und 14 Jahren durchgesetzt. Zudem wird es in bestimmten Fällen zu einer von fünf auf drei Jahre verkürzten Speicherung kommen und Regelungen zur datenschutzrechtlichen Verantwortlichkeit und Sperrung von Daten wurden aufgenommen. Ferner wurde der Übersichtlichkeit halber ein Ausführungserlass des Senators für Inneres aus dem Jahre 1985 überarbeitet und in angepasster Form in die KpS-Richtlinien integriert.

Im Zusammenhang mit der Überarbeitung der KpS-Richtlinien habe ich den Senator für Inneres und Sport auf verschiedene Probleme aufmerksam gemacht, die mir aus der Beschwerdepraxis bekannt sind. Dies betrifft z. B. die Speicherfristen für sog. personenbezogene Hinweise (PHW), wie etwa „bewaffnet“ oder „Konsument harter Drogen“. Die PHW werden zur Eigensicherung der Beamten im Zusammenhang mit Deliktseinträgen vergeben. Wird ein Deliktseintrag infolge späterer Delikte fortgespeichert, kann dies dazu führen, dass ein PHW über viele Jahre fortbesteht, obwohl es der tatsächlichen Situation des Betroffenen nicht mehr gerecht wird und fehlerhafte Polizeieinschätzungen fördert.

Auch wird nach meiner Erfahrung der PHW „psychisch auffällig“ verschiedentlich vergeben, ohne dass ein ärztliches Attest besteht (vgl. 30. JB, Ziff. 9.5). Eine derartige Vergabe durch nicht geschulte Beschäftigte bedeutet für die Betroffenen eine schwere Stigmatisierung. Die Betroffenen werden, wenn sie sich an die Polizei wenden, z. B. nicht mehr ernst genommen. Faktisch wird die Beweislast umgekehrt, indem den Betroffenen der Nachweis auferlegt wird, dass sie nicht „psychisch auffällig“ sind, was jedoch in der Praxis unmöglich ist. Damit wird das Recht der Betroffenen unterlaufen, unrichtige personenbezogene Daten berichtigen zu lassen.

Ein weiteres Problem ist, dass bei Ersuchen auswärtiger Dienststellen diese personenbezogen gespeichert werden. Da die auswärtigen Dienststellen den Verfahrensausgang, z. B. eine Einstellung des Verfahrens, nicht mitteilen und die Polizeien des Landes Bremen diesen nicht erfragen, kann eine solche Speicherung unter Umständen gravierende Folgen haben. So führte eine solche Speicherung zu einem negativen Ergebnis bei einer Zuverlässigkeitsüberprüfung nach dem Luftsicherheitsgesetz.

9.20 Beteiligung an Errichtungsanordnungen des Bundeskriminalamtes

Auch in diesem Jahr sind mir wieder vom Bundesministerium des Innern verschiedene Errichtungsanordnungen zu automatisierten Dateien mit personenbezogenen Daten beim Bundeskriminalamt (§ 34 BKAG) zur Stellungnahme gegenüber dem Senator für Inneres und Sport übersandt worden, u. a. zu „INPOL Fall Innere Sicherheit“ (IFIS), „WIKRI“ (zur Wirtschaftskriminalität), zur Antiterrordatei, zur „Verbunddatei Geldwäsche-Datei/Hinweisbearbeitung Geldwäsche“, zur „Verbunddatei Straftaten gegen ältere Menschen (SÄM)“, zur Datei „Korruption“ sowie für die Dateien „Gewalttäter rechts“, „Gewalttäter links“ und „Gewalttäter politisch motivierter Ausländerkriminalität“.

9.21 Verwaltungsvereinbarung mit der Zollverwaltung über Auskünfte nach § 17 Schwarzarbeitsbekämpfungsgesetz

Im September 2007 erfuhr ich, dass das Bundesministerium der Finanzen beabsichtigt, mit der Freien Hansestadt Bremen eine Verwaltungsvereinbarung über die Datenauskunft nach § 17 Schwarzarbeitsbekämpfungsgesetz zu schließen. Ich habe mir den Entwurf der Vereinbarung daraufhin übersenden lassen und hierzu Stellung genommen. In rechtlicher Hinsicht wies ich auf Abweichungen der Verwaltungsvereinbarung vom Wortlaut des Gesetzes hin, die eine Einschränkung, zum Teil aber auch eine Erweiterung der gesetzlichen Auskunftsmöglichkeiten bedeutet hätten. Daneben waren aus technischer Hinsicht verschiedene Aspekte der Datensicherheit nicht hinreichend beschrieben. Insoweit habe ich darum gebeten, weitere Informationen einzuholen. Schließlich habe ich auf verschiedene Schwierigkeiten hingewiesen, die sich bei der landesseitigen Umsetzung der Vorgaben der Verwaltungsvereinbarung zur Datensicherheit ergeben. Diese beabsichtige ich im Jahre 2008 weiter zu begleiten.

9.22 Zuverlässigkeitsüberprüfungen auf Einwilligungsbasis

Seitdem anlässlich der Fußball-WM 2006 im Rahmen der Akkreditierung massenhaft Zuverlässigkeitsüberprüfungen durch den Deutschen Fußball-Bund e. V. (DFB) stattgefunden haben, greifen diese Verfahren um sich. Im Jahr 2007 war ich verschiedentlich mit dieser Thematik konfrontiert, sei es, dass anlässlich des EU-Außenministertreffens in Bremen Mitarbeiter der Senatskanzlei, generell Fremdbeschäftigte bei der Deutschen Bundesbank oder Bewohner, Journalisten und andere Hilfskräfte anlässlich des G 8-Gipfels in Heiligendamm auf ihre „Zuverlässigkeit“ überprüft wurden.

Immer wieder muss betont werden, dass solche Zuverlässigkeitsüberprüfungen in das Grundrecht auf informationelle Selbstbestimmung eingreifen und nicht unter Umgehung gesetzlicher Vorschriften durchgeführt werden dürfen, denn außer etwa beim Bremischen Hafensicherheitsgesetz oder dem Luftsicherheitsgesetz oder dem Sicherheitsüberprüfungsgesetz gibt es keine klaren gesetzlichen Anforderungen an derartige Verfahren. Die allgemeinen Sicherheitsüberprüfungsgesetze des Bundes und der Länder sind in diesen Fällen regelmäßig nicht einschlägig und Einwilligungen der Betroffenen können die Überprüfungen, selbst wenn eine ausreichende Information über das Verfahren erfolgen würde, nicht rechtfertigen, da ihnen in der Regel die Freiwilligkeit als Wirksamkeitsvoraussetzung fehlt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich daher im Herbst 2007 in einer Entschließung gegen die Ausweitung der Zuverlässigkeitsüberprüfungen ausgesprochen und klare, notfalls gesetzliche Regelungen gefordert, die derartige Verfahren für die Betroffenen transparent machen und ihnen unverzichtbare Betroffenenrechte einräumt (vgl. Ziff. 21.11 dieses Berichts).

9.23 Heimliche Online-Durchsuchung privater Computer

Im Herbst 2006 lehnte ein Ermittlungsrichter beim Bundesgerichtshof den Antrag des Generalbundesanwaltes zur Durchführung einer „verdeckten Online-Durchsuchung“ zu Strafverfolgungszwecken ab. Der daraufhin vom Generalbundesanwalt angerufene Bundesgerichtshof (BGH) entschied am 31. Januar 2007 (AZ. StB 18/06), dass „verdeckte Online-Durchsuchungen“ zu Strafverfolgungszwecken mangels Rechtsgrundlage unzulässig sind.

Der Beschluss des BGH löste eine breite, öffentlich geführte Debatte über die Zulässigkeit und Notwendigkeit von heimlichen Online-Durchsuchungen aus. Im weiteren Verlauf wurde bekannt, dass dem Bundesministerium des Innern für das Haushaltsjahr 2007 bereits erhebliche Mittel für die Entwicklung der technischen Fähigkeiten zur Online-Durchsuchung bereitgestellt worden sind und die Nachrichtendienste auf Grundlage einer Dienstanweisung des vorigen Bundesinnenministers bereits seit längerem Online-Durchsuchungen durchführen. Eine in das nordrhein-westfälische Verfassungsschutzgesetz eingefügte Regelung für Online-Durchsuchungen wurde nach Inkrafttreten Anfang 2007 sogleich im Rahmen eines Verfassungsbeschwerdeverfahrens angegriffen. Die Entscheidung des Bundesverfassungsgerichts wird im Frühjahr 2008 erwartet. Es wurde eine zähe, politisch beeinflusste Diskussion unter Beteiligung des Bundesministerium des Innern, aber auch der Justiz über den Sinn und Zweck von Online-Durchsuchungen geführt, die Ausgestaltung einer gesetzlichen Regelung und die Notwendigkeit, die Regelung bereits vor der Entscheidung des Bundesverfassungsgerichts zu verabschieden bis hin zur Verfassungsänderung. Verschärft wurde diese Debatte durch einen im Sommer 2007 in Deutschland vereitelten Terroranschlag, obwohl die Vorgehensweise der Täter keine Argumente für den erfolgreichen Einsatz dieses Instrumentes lieferte, denn die Täter wechselten häufig ihre mobilen PC und loggten sich über fremde Funknetze ein.

Von Beginn an stieß die Online-Durchsuchung privater Computer auf Skepsis oder Ablehnung bei der rechtswissenschaftlichen und technikorientierten Literatur und bei Sachverständigen. Mit Entschließungen im März und Oktober 2007 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ihre entschieden ablehnende Haltung zum Ausdruck gebracht (vgl. Ziff. 21.9 dieses Berichts).

Heimliche Online-Durchsuchungen privater Computer stellen aufgrund der Vielzahl und Sensibilität der dort gespeicherten Daten (Fotografien, Tagebuch, Reiseberichte, persönlicher Schriftverkehr, Telefonrechnungen, Konto- oder Bewerbungsunterlagen) einen tiefen Eingriff in die Privatsphäre dar und können auch die Unverletzlichkeit der Wohnung und das Telekommunikationsgeheimnis beeinträchtigen. Die Maßnahme soll sich nicht auf eine Durchsuchung beschränken, sondern auch eine anhaltende Überwachung umfassen, um Passwörter zu erspähen und alle elektronischen Aktivitäten zu protokollieren. Sie soll sich neben Computern auch auf andere Kommunikations- und Datenverarbeitungssysteme, wie Mobiltelefone und PDAs (Personal Digital Assistant) erstrecken. In vernetzten Systemen können auch unverdächtige Nutzer mitbetroffen sein.

Dabei ist nach wie vor völlig ungeklärt, wie der verfassungsrechtlich absolut geschützte Kernbereich privater Lebenssphäre bei der Online-Durchsuchung durch technische Maßnahmen gewährleistet werden soll. Darüber hinaus steht die Beweiseignung der gewonnenen Erkenntnisse in Frage, da die eingesetzte Software die auf den Festplatten gespeicherten Daten unbemerkt manipulieren kann.

Schließlich führt bereits die Möglichkeit staatlicher Ausforschung des eigenen Computers mittels Schadsoftware („Bundestrojaner“) zu einem massiven Vertrauensverlust in die Sicherheit von Informationstechnik, insbesondere E-Government- und E-Commerce-Anwendungen und konterkariert hohe Aufwendungen für IT-Sicherheit in Staat und Wirtschaft. Ob eine angekündigte enge Zweckbindung auf die Bekämpfung des Terrorismus tatsächlich erfolgt und lange anhält, darf aufgrund der Erfahrungen der letzten Jahre ernsthaft bezweifelt werden. Auch dürften Terrorverdächtige, anders als der normale Bürger, Mittel und Wege finden, sich der Online-Durchsuchung zu entziehen. Diese wird daher voraussichtlich kein Mehr an Sicherheit bringen, aber sicher die Freiheiten der Bürger einschränken.

9.24 Bericht aus dem Arbeitskreis Sicherheit

Der Arbeitskreis Sicherheit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, in dem ich mitarbeite, beschäftige sich u. a. mit folgenden Themen: Konzeptionelle Weiterentwicklung des polizeilichen Informationssystems INPOL, Vorgangsbearbeitungssysteme bei den Polizeien der Länder, ein Gesichtserkennungssystem des Bundeskriminalamtes, der Stand der Einführung der Anti-Terror-Datei, die Gewährleistung des Kernbereichsschutzes und der Benachrichtigungspflicht bei verdeckten Ermittlungsmaßnahmen, die Ausweitung von sog. Zuverlässigkeitsüberprüfungen bei Akkreditierungsverfahren, datenschutzrechtliche Fragen bei der Durchführung der Operation „MIKADO“, Änderungen in Bezug auf Europol und das Schengener Informationssystem auf europäischer Ebene und die Zulässigkeit von Online-Durchsuchungen. In der Herbstsitzung wurde vor allem eine Stellungnahme zu der beim Bundesverfassungsgericht anhängigen Verfassungsbeschwerde gegen das Antiterrordateiengesetz abgestimmt. Ein weiteres Thema war erneut die Regelung zur Online-Durchsuchung im geplanten Bundeskriminalamtsgesetz, die Weiterentwicklung von INPOL, insbesondere die Protokollierung und die neuen Entwicklungen im Schengener Informationssystem und bei Europol, die zunehmend unmittelbare Auswirkungen auf das nationale Polizeirecht entfalten. Zudem widmete sich der Arbeitskreis erneut den verschiedenen Fallkonstellationen von Zuverlässigkeitsüberprüfungen auf Einwilligungsbasis und tauschte Erfahrungen zur Datenspeicherungspraxis durch den polizeilichen Staatsschutz aus.

10. Justiz

10.1 Prüfung von Gerichtsvollziehern

Im vergangenen Jahr habe ich die Datenverarbeitung der Gerichtsvollzieher verschiedener Amtsgerichte in Bremen und Bremerhaven geprüft. Prüfungsgegenstand waren die technischen und organisatorischen Maßnahmen nach § 7 Bremisches Datenschutzgesetz (BremDSG).

Bei den Prüfungen habe ich festgestellt, dass die in Bearbeitung befindlichen und abgeschlossenen Aufträge der Gerichtsvollzieher, allein in einem Fall waren es ca. 10.000 Vorgänge, häufig unzureichend gegen unbefugte Einsichtnahme geschützt aufbewahrt wurden. Ich habe gefordert, Abhilfe zu schaffen, z. B. durch Lagerung in abschließbaren Schränken.

Weiterhin fiel mir bei den Prüfungen auf, dass häufig Personen aus dem persönlichen Umfeld die PC der Gerichtsvollzieher für andere Zwecke nutzen und auch bei der Wartung und Betreuung der Systeme tätig sind. Support-Verträge mit entsprechenden DV-Dienstleistern bestehen in der Regel nicht. Zum Teil bestanden Zweifel an der fachlichen Eignung der Personen. Damit wurde den Regeln nach § 9 BremDSG nicht genügt. Der EDV-Support ist als Datenverarbeitung im Auftrag gemäß § 9 BremDSG zu qualifizieren. Hiernach ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Zudem muss ein schriftlicher Auftrag vorliegen, in welchem die technischen und organisatorischen Maßnahmen festgelegt werden. Darüber hinaus ist die beauftragte Person auf ihre Verschwiegenheit zu verpflichten.

Alle von mir geprüften Gerichtsvollzieher haben eine Datensicherung durchgeführt. Dabei muss die Lagerung der Datenträger für die Datensicherung teilweise verbessert werden. Eine offene Lagerung der Datensicherung stellt keine wirksame Datensicherung im Sinne von § 7 Abs. 4 Nr. 3, 4 und 7 BremDSG dar. Die Datenträger sind idealerweise extern (z. B. Bankschließfach), zumindest aber möglichst räumlich getrennt von der DV-Anlage und unter Verschluss zu lagern.

Einer der geprüften Gerichtsvollzieher führte die Datensicherung auf einer externen Festplatte durch. Die Daten (Gesamtdatenbestand) wurden dann auf ein Notebook übertragen. Das Notebook wird im Außendienst eingesetzt. Der Start des Notebooks war nicht einmal durch ein Passwort geschützt. Bei Verlust oder Diebstahl des Notebooks sind die Daten der Schuldner überhaupt nicht gegen unbefugten Zugriff und Weitergabe geschützt. Ich habe daher gefordert, das Notebook so zu konfigurieren, dass es nur nach Eingabe eines Passwortes bootet, eine manuelle Benutzeranmeldung nach dem Booten mit Benutzername und Passwort am System erfolgt und dass die Festplatte des Notebooks mit geeigneten Methoden verschlüsselt wird.

Außerdem wurde bei mehreren Gerichtsvollziehern am Dienst-PC das Internet teilweise mit Benutzerkonten mit Administratorberechtigung genutzt. Von Benutzerkonten mit Administratorberechtigung aus sollte niemals das Internet genutzt werden, da gefährliche Software (wie Viren oder Würmer) über fehlerhafte oder entsprechend manipulierte Web-Sites in das System eindringen und dann sofort mit der vollen Zugriffsberechtigung auf sämtliche Einstellungen, Programme und Daten auf dem PC zugreifen können. Ich habe gefordert, dass, wenn nicht auf die Internet-Nutzung per Dienst-PC komplett verzichtet werden kann, spezielle Benutzerkonten mit eingeschränkten Berechtigungen für die Internet-Nutzung eingerichtet werden. Nur von diesen Konten soll die Nutzung überhaupt möglich sein, aber Zugriff auf die Gerichtsvollzieher-Software oder die darin verarbeiteten Daten soll es nicht geben. Weiterhin muss nachgebessert werden, weil

Betriebssystem, Virenscanner und eingesetzte Firewall-Software nicht immer auf dem neuesten Stand sind.

Die vorgefundenen Mängel können an dieser Stelle nur exemplarisch geschildert werden. Ausführliche Feststellungen enthalten die jeweiligen Prüfberichte. Die Prüfungen habe ich zum Anlass genommen, in meinem Haus eine Orientierungshilfe für eine datenschutzkonforme Konfiguration und Nutzung von EDV-Systemen bei den Gerichtsvollziehern zu erarbeiten. Diese will ich in Abstimmung mit dem Justizressort über die Gerichte allen Gerichtsvollziehern zuleiten.

10.2 Neue Telekommunikationsanlage in der Justizvollzugsanstalt

Im Sommer 2006 wurde ich im Rahmen einer Eingabe gefragt, ob die bevorstehende Einführung einer neuen Telefonanlage in der Justizvollzugsanstalt Bremen datenschutzrechtlichen Anforderungen genüge.

Ich habe mir die Nutzungsmöglichkeiten des neuen Systems vor Ort unter datenschutzrechtlichen Gesichtspunkten erläutern lassen. Nach Prüfung und Genehmigung des Antrages eines Gefangenen wird durch die Zahlstelle ein Telefonkonto eingerichtet. Der Gefangene erhält von der Zahlstelle eine PIN-Nummer in einem verschlossenen Brief, die er jederzeit über das Telefon ändern kann. Dies ist unter dem Gesichtspunkt der Datensicherheit zu begrüßen.

Unter Vorwahl der PIN-Nummer kann der Gefangene über das Telefonsystem außerhalb der Verschlusszeiten telefonieren. In der Strafhaft können bestimmte Vorwahlnummern gesperrt werden, alle anderen Rufnummern sind frei wählbar. Besteht der begründete Verdacht, dass die Sicherheit und Ordnung der JVA Bremen gefährdet ist und daher in Einzelfällen Telefonate mitgehört werden müssen, ist das Mithören im Vorfeld unter Darlegung der Gründe durch die Anstaltsleitung zu genehmigen. Genehmigt die Anstaltsleitung das Mithören, wird der Gefangene vor Gesprächsbeginn über die beabsichtigte Überwachung benachrichtigt. Der Gesprächsteilnehmer wird per Autotextansage vor Gesprächsbeginn über die Mithörfunktion in Kenntnis gesetzt. Diese Vorgehensweise entspricht den gesetzlichen Vorgaben des § 32 Strafvollzugsgesetz.

Aus abrechnungstechnischen Gründen ist eine Speicherung der gewählten Rufnummern für 80 Tage erforderlich. Auf meine Anregung entfällt jedoch die Speicherung der letzten drei Stellen. Ich habe die Inbetriebnahme nach der Umsetzung meiner datenschutztechnischen Anregungen am Ende des Berichtsjahres für unbedenklich erklärt.

10.3 Beratung des Jugendstrafvollzugsgesetzes

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 31. Mai 2006 festgestellt, dass es keine verfassungsrechtlich ausreichende Rechtsgrundlage für den Jugendstrafvollzug gibt und daher eine eigenständige gesetzliche Normierung bis Ende 2007 geschaffen werden müsste.

Die datenschutzrechtlichen Anforderungen habe ich in einer Stellungnahme gegenüber dem Senator für Justiz und Verfassung formuliert. Auf meine Anregung empfahl der Rechtsausschuss der Bürgerschaft (Landtag) die Aufnahme einer Verschwiegenheitsverpflichtung für ehrenamtliche Mitarbeiter. Weitere datenschutzrechtliche Verbesserungsvorschläge fanden demgegenüber keine Berücksichtigung. Ich hatte insbesondere eine Änderung bezüglich der Offenbarungspflicht von Anstaltsärzten und -psychologen gegenüber der Anstaltsleitung angeregt. Die nunmehr in Kraft getretene Regelung sieht keine Interessensabwägung hinsichtlich der Offenbarungspflicht vor. Ich hatte vorgeschlagen, die Schweigepflichtdurchbrechung in das Ermessen der Anstaltsärzte und -psychologen zu stellen. Weiterhin hatte ich angeregt, zwischen den Regelungen zur Überwachung des Schriftverkehrs und der Telefongespräche eine Übereinstimmung herzustellen. Diese Änderungsvorschläge wurden mit Hinweis auf den weit fortgeschrittenen Stand des Gesetzgebungsverfahrens abgelehnt. Ich befürchte, die kritischen Regelungen würden einer verfassungsrechtlichen Überprüfung nicht standhalten. Der Rechtsausschuss erklärte sich bereit, die Punkte zu Beginn der nächsten Legislaturperiode bei der Novellierung des Strafvollzugsgesetzes erneut aufzugreifen.

10.4 Bericht aus dem Arbeitskreis Justiz

Der Arbeitskreis Justiz der Konferenz der Datenschutzbeauftragten des Bundes und der Länder tagte im Berichtsjahr zweimal. Schwerpunkte der Beratungen waren verfassungsrechtliche Fragen der heimlichen Online-Durchsuchung, Überprüfung von Telefonteilnehmern in Justizvollzugsanstalten, das Gesetz zur Neuregelung der Telefonüberwachung und anderer verdeckter Ermittlungsmaßnahmen, die elektronische Gerichtstafel und das Online-Abrufverfahren beim automatischen Grundbuch.

11. Gesundheit und Krankenversicherung

11.1 Mammographie-Screening

Die zentrale Stelle des Gesundheitsamtes Bremen ist für die Einladung von Frauen zwischen 50 und 69 Jahren unter anderem aus den Ländern Bremen und Niedersachsen zur Teilnahme am Mammographie-Screening zuständig.

Das dabei eingesetzte Softwareverfahren liest die erforderlichen Meldedaten ein und verarbeitet sie zur Abwicklung des Einladungswesens weiter. Zur Erweiterung des Einzugsbereichs der Zentralen Stelle aus Niedersachsen wurde eine Datenmigration der Region Nordwest erforderlich. Die Kassenärztliche Vereinigung Nordrhein (KVNo) entwickelte hierfür ein Migrationstool. Aufgrund der Unvollständigkeit der verwendeten Datensätze kam es zu Fehlern, durch die möglicherweise einige Frauen keine Einladung, eine Einladung zur falschen Screening-Einheit oder zu einem falschen Termin bekommen haben.

Zur Behebung dieser Fehler sollte ein Bereinigungstool von der KVNo entwickelt werden. Die Softwareentwickler der KVNo sollten z. B. Zugriff auf die Datenbank der Zentralen Stelle erhalten und Echtdaten zur Verfügung gestellt bekommen. Ich stellte die Erforderlichkeit eines solchen Zugriffs in Frage mit der Bitte um Prüfung einer alternativen Vorgehensweise. Darüber hinaus forderte ich eine Beschreibung der technischen und organisatorischen Maßnahmen, die den erforderlichen datenschutztechnischen Rahmen herstellen sollten. Hierzu gehörte auch eine Funktionsbeschreibung des Bereinigungstools und die Erteilung eines Auftrags an die KVNo, der den Anforderungen des § 80 SGB X genügt.

Bei meiner Einsichtnahme in die bestehenden Datenbestände der Zentralen Stelle entdeckte ich die Speicherung der extrem schützenswerten Kontrollnummer (Ordnungskriterium für das Krebsregister) zusammen mit Klartextdaten wie Geburtsmonat und -jahr, Postleitzahl und Ort. Gerade diese unzulässige Speicherung sollte für den Prozess der Datenbereinigung genutzt werden. Die Krebsfrüherkennungsrichtlinien sehen vor, dass die Kontrollnummern nur zusammen mit der über die Meldedaten gebildeten Screening-Identifikationsnummer, nicht aber zusammen mit personenidentifizierenden Daten im Klartext gespeichert werden dürfen. Ich habe deshalb die unverzügliche Löschung gefordert. Diese wurde inzwischen von der Zentralen Stelle bestätigt.

Es wurde dann von der Zentralen Stelle ein Konzept vorgelegt, gegen das ich keine grundsätzlichen Einwände hatte. Das Bereinigungstool stellt zum Vergleich der verschiedenen Teilnehmerinnen eine Maske zur Verfügung, in der ausschließlich die Übereinstimmung bzw. Nicht-Übereinstimmung der einzelnen Kontrollnummern optisch dargestellt wird. Es wird dann ein Wert angezeigt, der die Wahrscheinlichkeit der Übereinstimmung der zu vergleichenden Datensätze indiziert. Allerdings wurde von der Zentralen Stelle nach Vorlage des Konzeptes festgestellt, dass das Verfahren doch um die Verwendung einiger Klartextdaten erweitert werden muss, um die Bereinigung des Datenbestandes erfolgreich durchführen zu können. Nach Klärung der damit neu aufgetretenen datenschutzrechtlichen und -technischen Fragestellungen habe ich schließlich signalisiert, dass ich das Verfahren unter den gegebenen Umständen für vertretbar halte.

Mein Beratungsziel war es, die Behebung der Fehler zu ermöglichen, ohne gleichzeitig die Einhaltung der gerade für dieses sensible Projekt besonders entwickelten datenschutzrechtlichen Vorgaben zu gefährden.

Bereits während des Pilotprojektes Mammographie-Screening ab 2001 und anschließend auch beim Übergang in die Regelversorgung ab 2005 hatte ich eine engmaschige datenschutzrechtliche Begleitung geleistet. Bisher sind alle beim Mammographie-Screening auftretenden Fragestellungen und zu erstellenden Konzepte von mir sowohl in rechtlicher als auch in technischer Hinsicht geprüft und bewertet worden. Mit der Übernahme des Einladungswesen für die Bundesländer Niedersachsen, Hamburg und Sachsen-Anhalt durch das Gesundheitsamt Bremen begannen sich jedoch die ohnehin schon sehr zahl- und umfangreichen datenschutzrechtlichen Fragestellungen noch weiter zu häufen, so dass ich feststellen musste, dass eine derart intensive Begleitung des Mammographie-Screenings vor allem im Hinblick auf die angespannte personelle Situation in meiner Dienststelle von mir nicht mehr geleistet werden kann. Ich wandte mich daher an das Gesundheitsamt und bat darum, dass zukünftig in erster Linie der behördliche Datenschutzbeauftragte entsprechend seines in § 7 Abs. 2 BremDSG festgelegten gesetzlichen Auftrags die datenschutzrechtliche Begleitung des Projektes wahrnehmen solle und verwies auf die Möglichkeit, dabei externen Sachverstand hinzuzuziehen.

Im Juli erhielt ich eine Einladung in das Referenzzentrum Mammographie Bremen, wo von einer Vertreterin des Krebsregisters in Niedersachsen ein neues Konzept zur Evaluation des Screening-Programms vorgestellt wurde. Das Konzept setzt umfangreiche, weit über die Festlegungen in den Krebsfrüherkennungsrichtlinien hinausgehende Datenübermittlungen zwischen der Zentralen Stelle für das Einladungswesen, den Krebsregistern, den Screening-Einheiten und dem Referenzzentrum voraus. Beispielsweise sollten in der Zentralen Stelle für das Einladungswesen zukünftig neben der Kontrollnummer und der Screening-ID auch Postleitzahl, Wohnort, Geburtsmonat und Geburtsjahr der eingeladenen Frauen dauerhaft gespeichert und an die Krebsregister übermittelt werden. Vom Krebsregister sollten das Datum der Krebsdiagnose und weitere histologische Daten an die Zentrale Stelle übermittelt werden. Zudem sollte zum Zwecke der Mortalitätsevaluation das Datum und Ergebnis der letzten Screening-Untersuchung der an Krebs erkrankten Frauen durch die Screening-Einheit an das Krebsregister gemeldet werden.

Eine Umsetzung dieses Konzeptes würde eine erhebliche Absenkung des im Screening-Programm erreichten Datenschutzniveaus bedeuten. Eine Rechtsgrundlage für die zusätzlichen geplanten Datenübermittlungen, die zudem überwiegend im Widerspruch zu den Regelungen des Bremischen Krebsregistergesetzes stehen, wäre nicht vorhanden. Außerdem kann bei diesem Verfahren eine Anonymität der betroffenen Frauen mit ihren Befunddaten in der Zentralen Stelle für das Einladungswesen nicht mehr hinreichend gewährleistet werden. Das aktuell in den Krebsfrüherkennungsrichtlinien geltende Einwilligungserfordernis der betroffenen Frau für die Übermittlung von Befunddaten würde ausgehebelt. Die Erforderlichkeit einer Rechtsgrundlage für die geplanten Datenübermittlungen ist von der Kooperationsgemeinschaft Mammographie lange Zeit ignoriert worden. Zurzeit setzt die Kooperationsgemeinschaft sich für eine Abbildung ihres im Zeitraum von Juli bis Dezember mehrfach geänderten Konzeptes in den Krebsfrüherkennungsrichtlinien ein. Bezüglich der Krebsfrüherkennungsrichtlinien, die vom Bundesausschuss der Ärzte und Krankenkassen erlassen werden, ist im Hinblick auf die Wesentlichkeitsrechtsprechung des Bundesverfassungsgerichts bereits fraglich, ob solche mit stark abgeleiteter demokratischer Legitimation verabschiedeten Normwerke überhaupt die gesetzlich Versicherten binden und ihre Grundrechte einschränken können. Die nicht gesetzlich Versicherten können von den im Bereich der

sozialen Selbstverwaltung erlassenen untergesetzlichen Normen jedenfalls nicht erfasst werden. Meiner Ansicht nach könnte eine Rechtsgrundlage hierfür nur durch ein Gesetz oder eine Einwilligungserklärung der betroffenen Frauen geschaffen werden. Die Beratungen zu diesem Punkt dauern noch an.

11.2 Prüfung im Bereich Krankengeld der AOK Bremen/Bremerhaven

Im Oktober des Berichtsjahres habe ich Maßnahmen zur Zugangs- und Zugriffskontrolle in Bezug auf die für das Krankengeldfallmanagement eingesetzte Software geprüft.

Dabei habe ich mehrere datenschutzrechtliche Verstöße festgestellt. Zum Teil werden seit Jahren geltende grundlegende Standards nicht eingehalten. Das Verfahren ermöglicht keine Einstellung von Kennwörtern, wie beispielsweise technisch erzwungene Passwortlängen, Vorgaben zur Komplexität und zur Historie. Auch organisatorische Vorgaben gibt es hierzu nicht. Statt dessen müssen die Passwörter der Teamleitungen zur Verfügung gestellt werden. Diese führen eine Passwörterliste und können mit den Passwörtern der jeweiligen Sachbearbeitung auf die Daten des Fachverfahrens zugreifen. Die Bekanntgabe von Passwörtern verstößt gegen Nr. 5 der Anlage zu § 78 a SGB X, Eingabekontrolle. Für Vertretungsfälle wird verlangt, das persönliche Passwort ebenfalls der Vertretung bekannt zu geben. Abgesehen von der mangelnden Qualität der Passwörter und dem geringen Schutz, den nicht mehr geheim gehaltene Passwörter nur noch bieten, ist für den Fall einer Revision oder datenschutzrechtlichen Prüfung nicht mehr nachvollziehbar, wer wann auf welche Daten zugegriffen hat. Eine mir im Nachgang zur Prüfung per Mail unverschlüsselt übermittelte Passwörterliste genügt den Qualitätsanforderungen ebenfalls nicht. Darüber hinaus bleiben durch die Übermittlung der Liste im Klartext die Anforderungen der Transportkontrolle unberücksichtigt. Da es sich um den Zugriff auf Gesundheitsdaten handelt, ist der Schutz dieser Daten entsprechend dem Stand der Technik durch technische Maßnahmen zu gewährleisten (§ 78 a SGB X).

Die Software zum Krankengeldfallmanagement bietet keine Möglichkeit der Protokollierung, d. h., selbst wenn es eine datenschutzgerechte Zugangskontrolle zum System gäbe, würde die Möglichkeit, darauf eine Revision aufzubauen, von der Software nicht bereitgestellt.

Die Software zum Krankengeldfallmanagement stellt darüber hinaus keine Rollendifferenzierung zur Verfügung. Eine genaue Einstellung, wer mit welchen Rechten auf welche Daten zugreifen darf, gibt es nicht. Damit können z. B. die Sachbearbeiterinnen/Sachbearbeiter an ihren Arbeitsplätzen nicht sicher sein, dass die Daten der Fälle, die sie verantwortlich bearbeiten, auch nur von ihnen selbst verändert werden können.

Darüber hinaus existiert an den Arbeitsplätzen ein Vollzugriff auf die Datenbank, in denen Diagnosedaten der AOK-Mitglieder teilweise über einen Zeitraum von 25 Jahren gespeichert sind.

Die festgestellten Zustände sind wie folgt zu bewerten:

Nach der Verpflichtung zur Wahrung des Sozialgeheimnisses nach § 35 SGB I hat jeder Anspruch darauf, dass die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden (Sozialgeheimnis). Die Wahrung des Sozialgeheimnisses umfasst die Verpflichtung, auch innerhalb des Leistungsträgers, also auch innerhalb der AOK, sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden. § 284 Abs. 3 Satz 1 SGB V erlaubt eine Nutzung von Sozialdaten für die in Absatz 1 aufgelisteten Zwecke nur in dem jeweils erforderlichen Umfang. Die Möglichkeit des Vollzugriffs auf sämtliche Diagnosedaten eines Versicherten durch die im Bereich Krankengeldfallmanagement tätigen Mitarbeiter über einen unbegrenzten Zeitraum ist für die Erfüllung der Aufgaben des Krankengeldfallmanagements nicht erforderlich und stellt deshalb einen Verstoß gegen die oben

genannten Vorschriften dar. Nach § 84 Abs. 2 Satz 2 SGB X sind Sozialdaten zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Daher sind für die Speicherung von Diagnosedaten begründete Löschfristen festzulegen und die Daten umgehend zu löschen, sofern sie für den Zweck der Aufgabenerfüllung nicht mehr erforderlich sind.

Das Verfahren zum Krankengeldfallmanagement stellt kein Rollenkonzept, keine angemessene Zugangskontrolle (Passwortrestriktionen) und keine erforderliche Protokollierung (§ 78 a SGB X, Anlage Nr. 5) zur Verfügung. Es entspricht nicht dem erforderlichen Stand der Technik. Ich habe der AOK Bremen/Bremerhaven mitgeteilt, dass der Betrieb des Verfahrens in dieser Form unzulässig ist und sie aufgefordert, umgehend die Zugriffe auf Diagnosedaten zu begrenzen, Fristen für das Sperren und Löschen dieser Daten festzulegen und das Verfahren zur Passwortgestaltung zu dokumentieren, insbesondere hinsichtlich der Passwortrestriktionen und der Gewährleistung der Geheimhaltung.

11.3 Elektronische Gesundheitskarte

Der Rollout der elektronischen Gesundheitskarte ist nunmehr für das zweite Quartal 2008 geplant. Zu diesem Zeitpunkt soll die Karte mit einem Foto, aber noch ohne die Anwendungen e-Rezept, Notfalldatensatz, Arztbrief, elektronische Patientenakte und Patientenfach ausgestattet sein, durch die die Karte zu einem späteren Zeitpunkt erweitert werden sollen.

Zur Erinnerung: Bremen hat sich aus dem Anwendungstest verabschiedet (vgl. 29. JB, Ziff. 11.1). Gleichwohl muss ich die Entwicklung natürlich weiter beobachten.

Mittlerweile haben fast alle sieben Testregionen Gesundheitskarten ausgegeben und mit der Testung (Release 1, offline) begonnen. Unter anderem traten bei der Testung Probleme mit dem Heilberufeausweis auf, der wegen fehlerhafter Codierung ausgetauscht werden musste. Teilweise gab es auch Widerstand von Seiten der Ärzte.

Die Klärung einiger entscheidender Grundsatzfragen steht zurzeit noch aus, wie beispielsweise die Festlegung einer verantwortlichen Stelle im Gesamtsystem und der entsprechenden Kontrollzuständigkeit. Weitere offene Fragen betreffen die Möglichkeit der Wahrnehmung der Betroffenenrechte von zu Hause aus und die Einwilligungsfähigkeit Minderjähriger in der konkreten praktischen Umsetzung.

11.4 Bericht aus dem Arbeitskreis Gesundheit und Soziales

Ich arbeite im AK Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit, unter anderen wurden folgende Themen beraten:

Elektronische Gesundheitskarte, Mammographie-Screening, Grundsicherung für Arbeitssuchende im SGB II, Programm Oscare der AOK, Datenerhebung in der gesetzlichen Rentenversicherung und Maßnahmen zum Schutz von Kindern vor Misshandlung und Verwahrlosung.

11.5 Kindeswohl

Die gesundheitsrechtlichen Aspekte dieses Themas sind mit den sozialrechtlichen zusammengefasst unter Ziff. 12.3 dieses Berichts zu finden.

12. Arbeit und Soziales

12.1 Datenschutz in der BAgIS und der ARGE Job Center Bremerhaven

Nachdem sich meine Aktivitäten im Hinblick auf die BAgIS im Jahr 2006 noch fast ausschließlich auf die Bearbeitung der zahlreichen Eingaben von Hilfeempfängern beschränkten, bin ich erfreut, für das Jahr 2007 berichten zu können, dass sich die Zusammenarbeit mit den Mitarbeitern der BAgIS wesentlich verbessert hat. Den Grund dafür sehe ich vor allem in der Durchführung von zwei Fortbildungsveranstaltungen im Aus- und Fortbildungszentrum zum Thema Sozialdatenschutz im Mai 2007, an der alle Teamleiterinnen/Teamleiter der BAgIS teilgenommen haben. Dadurch konnte ich erreichen, dass ich in letzter Zeit vermehrt auch von Mitarbeitern der BAgIS, die mir seitdem in Fragen des Datenschutzes weitaus sensibilisierter erscheinen, sowohl Anfragen zu datenschutzgerechtem eigenen Verhalten als auch Beschwerden bei Datenschutzverstößen anderer erhalte.

Hinzu kommt, dass sowohl die BAgIS als auch die ARGE Job Center Bremerhaven in diesem Jahr behördliche Datenschutzbeauftragte bestellt haben, damit stehen kompetente Ansprechpartner zur Verfügung. Erwähnen möchte ich außerdem, dass der stellvertretende Leiter einer Geschäftsstelle der BAgIS mich nach der Fortbildungsveranstaltung zu einem Informationsbesuch eingeladen hat, bei dem er mir sehr detailliert die tägliche Arbeit und die daraus resultierenden Probleme, auch in datenschutzrechtlicher Hinsicht, erläutert hat. Auf der Basis der dort gewonnenen Erkenntnisse habe ich eine Reihe von Verbesserungsvorschlägen gemacht, deren Umsetzung zurzeit geprüft wird.

Dennoch möchte ich nicht verhehlen, dass mich auch weiterhin viele Eingaben von Hilfeempfängern erreichen, von denen ich eine kleine Auswahl gern schildern möchte:

Im Februar 2007 wandte sich ein Hilfeempfänger an mich und teilte mit, von der BAgIS aufgefordert worden zu sein, eine Eingliederungsvereinbarung zu unterzeichnen, in der er sich unter anderem zur Entbindung seiner Ärzte von der Schweigepflicht verpflichtete. Als er sich weigerte, die Vereinbarung zu unterzeichnen, habe die BAgIS diese per Verwaltungsakt in Kraft gesetzt. Ich erläuterte der BAgIS, dass es keine Rechtsgrundlage gibt, die einen Hilfeempfänger verpflichtet, eine ärztliche Schweigepflichtentbindungserklärung abzugeben. Nach § 67 b Abs. 2 Satz 2 SGB X ist die Einwilligung des Betroffenen nur wirksam, wenn sie auf dessen freier Entscheidung beruht. Eine Verpflichtung dazu ist daher unzulässig, sie sei daher zurückzunehmen. Die zuständige Teamleiterin der BAgIS bestätigte mir dann, eine entsprechende Verpflichtung auch zukünftig zu unterlassen.

Im Juni 2007 schilderte mir eine Hilfeempfängerin, die für den Monat Juni einen Werkvertrag abgeschlossen hatte, dass ihre Sachbearbeiterin der BAgIS sich ohne vorherige Rücksprache an die Auftraggeberin gewandt hatte, um einen Zeitpunkt für die Auszahlung des Honorars zu vereinbaren, so dass dadurch der Auftraggeberin die Hilfebedürtigkeit ihrer Auftragnehmerin zur Kenntnis gelangt ist. Ich wies die BAgIS darauf hin, dass dieses Vorgehen sowohl einen Verstoß gegen die Verpflichtung zur Wahrung des Sozialgeheimnisses nach § 35 Abs. 1 SGB I als auch gegen den Grundsatz der Datenerhebung beim Betroffenen nach § 67 Abs. 2 SGB X darstellt, woraufhin mir die Geschäftsstellenleiterin der BAgIS versicherte, alle Mitarbeiter über die Unzulässigkeit eines solchen Vorgehens informiert zu haben, um entsprechende Vorfälle zukünftig zu unterbinden.

Immer wieder erreichen mich Eingaben von Bürgern bezüglich der Praxis der BAgIS zur Anforderung von Kontoauszügen. Teilweise fordert die BAgIS eine lückenlose Einreichung von Kontoauszügen, die dann in Kopie zur Akte genommen werden. Zur datenschutzgerechten Ausgestaltung der Anforderung von Kontoauszügen bei der Beantragung von Sozialleistungen sind in Zusammenarbeit einiger

Landesbeauftragter für Datenschutz „Gemeinsame Hinweise“ erstellt worden. Danach ist eine Anforderung von Kontoauszügen lediglich der letzten drei bis sechs Monate nur bei der erstmaligen Beantragung von Sozialleistungen und während des laufenden Hilfebezugs erst wieder nach Ablauf von zwölf Monaten oder wenn dies erforderlich ist, zur Klärung einer konkreten Frage zur Einkommens- und Vermögenssituation oder bei einem konkreten Verdacht auf Sozialleistungsbetrug zulässig. Dabei ist das Schwärzen einzelner Buchungstexte, insbesondere Sollbuchungen über Beträge bis 50 €, grundsätzlich zulässig, worauf die Hilfeempfänger bereits bei der Anforderung der Kontoauszüge hinzuweisen sind. Die insoweit erhobenen Daten dürfen von der BAgIS zwar erhoben, aber nicht gespeichert werden, so dass eine Einsichtnahme vorgenommen werden kann, nicht aber eine Kopie der Kontoauszüge zur Akte genommen werden darf. Ich bat die Datenschutzbeauftragte der BAgIS darum sicherzustellen, dass diese Hinweise in allen Geschäftsstellen beachtet würden. Sie informierte daraufhin alle Führungskräfte und Teamleiterinnen/Teamleiter der BAgIS und bat um Beachtung der „Gemeinsamen Hinweise“.

Ein weiterer Aspekt, der immer wieder Anlass zu Beschwerden bietet, ist die mangelnde Vertraulichkeit sowohl in den Wartebereichen als auch in den Sachbearbeiterzimmern der BAgIS. Sehr häufig melden sich Hilfeempfänger, die berichten, dass in den Geschäftsstellen bereits bei der Anmeldung Sozialdaten offenbart werden müssen, die im Wartebereich von den anderen Kunden mitgehört werden könnten. Auch in den Sachbearbeiterzimmern würden häufig mehrere Hilfeempfänger gleichzeitig beraten, so dass es auch dort zur Offenbarung von Sozialdaten komme. Meine Hinweise an die BAgIS, dass die Verpflichtung zur Wahrung des Sozialgeheimnisses die Offenbarung von Sozialdaten sowohl gegenüber anderen Hilfeempfängern als auch gegenüber anderen nicht zuständigen Sachbearbeitern verbietet, werden von der BAgIS meistens damit beantwortet, dass die räumliche Situation nicht zu ändern sei, den Hilfeempfängern auf Nachfrage aber selbstverständlich eine Beratung in einem Einzelzimmer ermöglicht werde. Meine Erfahrungen mit Hilfeempfängern der BAgIS haben jedoch gezeigt, dass diese sich oftmals verpflichtet fühlen, trotz fehlender Vertraulichkeit Angaben zu machen. Obwohl diese Situation als sehr unangenehm empfunden wird, trauen sie sich nicht oder sind sich der Möglichkeit nicht bewusst, darauf zu bestehen, ihre Sozialdaten nicht im Beisein anderer offenbaren zu müssen. Ich habe daher darauf hingewirkt, dass in den betroffenen Geschäftsstellen der BAgIS wenigstens Hinweisschilder installiert werden, die über die Möglichkeit der Beratung in einem Einzelbüro aufklären.

Im Oktober wandte sich eine Kundin der ARGE Job Center Bremerhaven an mich und teilte mit, dass die ARGE ihrem geschiedenen Ehemann telefonisch Auskünfte erteilt habe. Unter anderem habe dieser dabei erfahren, dass sie neben einem gemeinsamen Sohn noch ein weiteres Kind mit einem anderen Mann habe. Sie selbst habe sich auch schon gewundert, dass bei telefonischen Auskünften durch die ARGE keinerlei Identitätsprüfung erfolge. Ich wies die ARGE darauf hin, dass diese Praxis nicht den Anforderungen an die Verpflichtung zur Wahrung des Sozialgeheimnisses genügt, wonach jeder Anspruch darauf hat, dass die ihn betreffenden Sozialdaten nicht unbefugt übermittelt werden. Von dort bekam ich die Antwort, dass die Mitarbeiter aufgrund dieses Vorfalls auf die Verpflichtung zur Einhaltung der Datenschutzbestimmungen der Bundesagentur für Arbeit zur Auskunft über Sozialdaten an Dritte hingewiesen worden sind, wonach bei einer Auskunft über Sozialdaten an Dritte die Berechtigung zum Empfang der Daten zweifelsfrei nachgewiesen werden muss. Dies hat in der Regel durch eine schriftliche Vollmacht zu geschehen, die eindeutig zum Empfang der verlangten Auskunft berechtigt. Anderenfalls hat eine Auskunftserteilung zu unterbleiben. Bei einer

Auskunftserteilung am Telefon sind zur eindeutigen Feststellung der Identität des Anrufers gezielte Fragen nach Identifikationsmerkmalen wie Vor- und Zuname, Geburtsdatum, Kunden- oder Kontonummer sowie der Anschrift erforderlich, eine Auskunft an Dritte zu dokumentieren.

12.2 Bewerbungen: Prüfung bei einem Maßnahmeträger im Bereich SGB II

Im August 2007 führte ich eine Datenschutzprüfung bei einem Maßnahmeträger im Bereich SGB II durch. Bei dem Träger handelt es sich um eine GmbH, die sowohl Bewerbungstrainings für Hilfeempfänger als auch Zeitarbeitsvermittlung betreibt. Die Teilnehmer am Bewerbungscenter verpflichten sich im Rahmen einer Eingliederungsvereinbarung gegenüber der BAgIS zur Teilnahme am Bewerbungscenter für einen Zeitraum von vier bis sechs Monaten. In der GmbH werden die Teilnehmerdaten im Aufnahmegespräch anhand eines Bewerberprofilbogens elektronisch erfasst. Die Teilnehmer des Bewerbungscenters werden bei der Erstellung von schriftlichen Bewerbungsunterlagen an Computerarbeitsplätzen von Dozenten geschult und beraten. Die erstellten Bewerbungen werden von den Dozenten Korrektur gelesen und anschließend versandt. Die Antwort auf die Online-Bewerbungen laufen auf den von den Dozenten genutzten Rechnern auf, werden ausgedruckt und den entsprechenden Bewerberinnen/ Bewerbern zur Verfügung gestellt.

Den Teilnehmern am Bewerbungscenter wird eine Einwilligungserklärung vorgelegt, mit der sie sich einverstanden erklären können, dass ihnen von den Dozenten des Bewerbungscenters Stellen aus dem Bereich Zeitarbeitsvermittlung angeboten werden. Wenn diese Einwilligungserklärung nicht unterzeichnet wird, wird dies der BAgIS mitgeteilt.

Die GmbH hat einen Datenschutzbeauftragten bestellt. In seiner Bestellungsurkunde war als zuständige Aufsichtsbehörde fälschlicherweise nicht der Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen genannt.

Da eine Rechtsgrundlage für die Datenerhebung bei den Teilnehmern nicht vorhanden ist, stellte ich in rechtlicher Hinsicht insoweit fest, dass sämtliche Datenerhebungen durch die GmbH nur auf Einwilligungsbasis stattfinden können. Datenerhebungen nach § 3 Abs. 3 BDSG stellen sowohl die Einsichtnahme in die Bewerbungsunterlagen durch die Dozenten, die Kenntnisnahme der Antworten auf Online-Bewerbungen als auch die Datenerhebung anhand des Bewerberprofilbogens dar. Ich forderte daher die Erstellung eines Formulars für eine Einwilligungserklärung zur Datenerhebung, das den Anforderungen des § 4 a BDSG genügt, also unter anderem die unterschiedlichen Zwecke der einzelnen Datenerhebungen klar erläutert, wie zum einen den Zweck der Hilfe bei der Erstellung von Bewerbungsunterlagen und zum anderen den Zweck der Vermittlung in Zeitarbeit.

Zudem stellte ich fest, dass die Bestellungsurkunde für den betrieblichen Datenschutzbeauftragten nicht den gesetzlichen Anforderungen genügt. Sie muss von beiden Parteien unterschrieben werden und u. a. eine detaillierte Aufgabenbeschreibung enthalten. Weiterhin muss darin eine ausreichende Konkretisierung der Verpflichtung der verantwortlichen Stelle erfolgen, die für eine konkrete Erfüllung der Aufgaben des Beauftragten erforderliche personelle und materielle Unterstützung zu gewähren hat. Die Nennung der zuständigen obersten Aufsichtsbehörde musste korrigiert werden.

In technischer Hinsicht sind folgende Aspekte von Bedeutung: In dem von mir geprüften Bewerbungscenter standen für die Erstellung von schriftlichen Bewerbungsunterlagen mehrere miteinander vernetzte Rechner zur Verfügung. Die Kunden und Kundinnen konnten u. a. Microsoft-Standardprodukte nutzen und über bereitgestellte Links zu Jobbörsen Informationen abrufen.

Der Zugang zu den Rechnern ist während der Öffnungszeiten des Bewerbungscenters offen, es besteht ein Passwortschutz zum Starten der Rechner, der durch die Dozentin und den Dozenten

gewährleistet wird. Sind die Rechner einmal gestartet, können verschiedene Kunden ohne nochmalige Anmeldung am Betriebssystem an den Rechnern arbeiten. Die erarbeiteten Bewerbungsunterlagen werden geschützt in einem persönlichen Verzeichnis abgelegt.

Die vorgefundenen Einstellungen sind vor dem Hintergrund, dass für die Kunden und Kundinnen ein unkomplizierter und schneller Zugang zu den Rechnern möglich sein muss, akzeptabel.

Neben der Erstellung von Bewerbungsunterlagen wurde den Kunden und Kundinnen die Möglichkeit der Versendung von Online-Bewerbungen zur Verfügung gestellt. Der Dozent und die Dozentin konnten die Bewerbungen über eine Mailsoftware versenden, etwaige Antworten liefen dort wieder auf. Die Antwort auf eine Bewerbung wurde dann ausgedruckt und den entsprechenden Bewerbern und Bewerberinnen zur Verfügung gestellt. Die Daten wurden unverschlüsselt übermittelt. Dieses Verfahren wurde datenschutzgerechter gestaltet. Es wurde für jede Kundin und jeden Kunden ein eigener E-Mail-Account bei einem vom Kunden ausgewählten Anbieter eingerichtet. Die Antworten auf Online-Bewerbungen gehen also direkt auf dem privaten E-Mail-Account ein.

Die unverschlüsselte Übersendung von Bewerberdaten über das Internet bietet keinen ausreichenden Schutz der übermittelten Daten. Da eine schriftliche Bewerbung häufig nicht mehr möglich ist und die Firmen in den seltensten Fällen die Möglichkeit einer Verschlüsselung anbieten, ist das Problem allein im Bewerbungscenter nicht zu lösen.

Für den weiteren Schutz der Dokumente ist die Absicherung der Rechner auf der Ebene des Betriebssystems und die Konfiguration von Sicherheitsmechanismen gegenüber nicht autorisierten Zugriffen aus dem Internet wichtig. Die Einrichtung und Administration der Rechner und der Netzinfrastruktur ist in Auftrag gegeben worden. Der hierzu schriftlich erteilte Auftrag, der auch die vom Auftragnehmer zu implementierenden Sicherheitsmaßnahmen definieren muss (vgl. § 9 BDSG nebst Anlage), wurde nach Redaktionsschluss vorgelegt. Es wurde eine Dokumentation über die Absicherung der Internetzugänge und ein EDV-Service-Vertrag übersandt. Zur Kontrollierbarkeit und Revision der durch den Auftagnehmer am System vorgenommenen Tätigkeiten wurden keine Aussagen getroffen. Eine Bewertung meinerseits steht noch aus.

12.3 Kindeswohl

Im Berichtsjahr wurden verschiedene Maßnahmen ergriffen, die dazu dienen sollen, Kindesvernachlässigungen und –misshandlungen zu verhindern. Ich wurde dabei in der Regel beteiligt, habe die Gesetzgebung unter den im Vorwort genannten Prämissen (vgl. Ziff. 1.9 dieses Berichts) begleitet und meine Beratung des Verwaltungshandelns wie der Verwaltungsvorschriften am geltenden Recht ausgerichtet.

12.3.1 Kindeswohlgesetz

Im März 2007 wurde mir der Entwurf des Gesetzes zur Sicherung des Kindeswohls zur Stellungnahme zur Verfügung gestellt. Ziel dieses Gesetzentwurfs ist der Aufbau eines flächendeckenden Einladungswesens zu den Früherkennungsuntersuchungen U5 bis U9. Die Zentrale Stelle für das Einladungswesen für das Land Bremen soll beim Gesundheitsamt Bremen eingerichtet werden. Dies soll von der Meldebehörde regelmäßig die erforderlichen Daten erhalten, um alle gesetzlichen Vertreter der Kinder, dessen Früherkennungsuntersuchungen U5 bis U9 bevorstehen, zur Teilnahme des Kindes an der Früherkennungsuntersuchung bei einem niedergelassenen Arzt schriftlich einzuladen. Die niedergelassenen Ärzte, die eine entsprechende Früherkennungsuntersuchung durchgeführt haben, sollen verpflichtet werden, dem Gesundheitsamt Bremen eine schriftliche Bestätigung der Teilnahme des Kindes zu übermitteln. Die gesetzlichen Vertreter der Kinder, für die nach Ablauf einer angemessenen Frist keine Bestätigung über die Teilnahme eingegangen ist, sollen eine schriftliche Erinnerung erhalten. Erfolgt nach einer weiteren angemessenen Frist noch immer keine Teilnahmebestätigung eines Arztes, so soll das Gesundheitsamt gezielt Kontakt mit dem gesetzlichen Vertreter aufnehmen. Dabei kann es einen Hausbesuch ankündigen und gleichzeitig die Durchführung der Früherkennungsuntersuchung während des Hausbesuchs anbieten. Für den Fall, dass die Durchführung der Früherkennungsuntersuchung durch den gesetzlichen Vertreter abgelehnt wird, soll eine Meldung an das Jugendamt erfolgen.

Angesichts der kurzen Frist zur Stellungnahme von zwei Tagen sah ich keine Möglichkeit, grundsätzlichen datenschutz- und verfassungsrechtlichen Fragen nachzugehen. In diesem Sinne wäre meines Erachtens vor Erlass des Gesetzes zu prüfen, ob ein derartig eng gewählter Betreuungsrahmen mit den verfassungsrechtlich garantierten Elternrechten in Einklang steht, da auch weiterhin keine Pflicht zur Teilnahme an den Früherkennungsuntersuchungen besteht. Zudem ist mir nicht bekannt, ob es Untersuchungen gibt, die belegen, dass es eine nennenswerte Dunkelziffer von Kindeswohlgefährdungen gibt, die mit diesem gesetzlich vorgesehenen Verfahren aufgeklärt werden könnten. Der Fall Kevin, der in Bremen Auslöser für die Einführung des flächendeckenden Einladungswesens gewesen ist, erscheint jedenfalls nicht als geeignetes Beispiel, da den zuständigen Behörden die Verhältnisse bekannt waren. Klärungsbedürftig wäre weiterhin gewesen, ob die gegenwärtigen Regelungen im Sozialgesetzbuch sowie die nach dem Tod von Kevin eingeleitete Anpassung und Neuausrichtung organisatorischer und informativer Strukturen in den zuständigen Behörden nicht bereits ausreichen, Kindeswohlgefährdungen besser zu erkennen und zu beseitigen, um nur einige Überlegungen zu nennen.

Unter Auslassung dieser Aspekte machte ich Vorschläge, damit die Meldepflicht der Ärzte sich auf die unbedingt notwendigen Daten beschränken kann. Weiter schlug ich vor, bei der Rückmeldung des Arztes als auch nach Versand der Erinnerung an die Eltern in der Regelung konkrete Fristen zu benennen. Zudem wies ich darauf hin, dass in den Fällen, in denen Ärzte ihrer Mitteilungspflicht nicht oder nicht rechtzeitig nachkommen, die Nachteile von den betroffenen Familien zu tragen wären, weshalb für diese Fälle eine Ausweichklausel, die dem Gesundheitsamt eine andere Verfahrensweise ermöglicht, geschaffen werden sollte.

Anschließend wurde mir ein überarbeiteter Gesetzentwurf zugeleitet, der meine Änderungsvorschläge nur zu einem geringen Teil aufnahm. Die oben genannten Anmerkungen wurden nicht berücksichtigt. Am 1. Mai 2007 trat das Gesetz zur Sicherung des Kindeswohls und zum Schutz von Kindesvernachlässigung (Kindeswohlgesetz – KiWG) in Kraft (Brem.GBl. 2007, S. 317).

Anfang Juni fand eine erste Zusammenkunft zur Umsetzung des Kindeswohls im Hause der Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales statt. In diesem Rahmen beriet ich die Gestaltung der Einladungs- und Erinnerungsschreiben. Im Rahmen der Besprechung kam auch die Frage auf, wie eine Meldung durch die Ärzte erfolgen soll, wenn das dafür vorgesehene, bereits mit den Daten des Kindes versehene Formular für die Meldung an das Gesundheitsamt von den Eltern nicht zum Untersuchungstermin mitgebracht würde. Mit dem Hinweis auf einen erhöhten Verwaltungsaufwand weigerten sich die Vertreter der Ärzte zunächst, die Daten des Kindes vor Ort in ein Formular einzutragen. Es wurde vorgeschlagen, in diesen Fällen unter Verwendung der Daten auf der Krankenversichertenkarte des Kindes ein Rezeptformular auszudrucken und statt des Formulars zu übermitteln. Obwohl ich darauf hinwies, dass die Übermittlung der auf der Versichertenkarte gespeicherten Daten an das Gesundheitsamt zur Aufgabenerfüllung nicht erforderlich sei und damit einen Verstoß gegen den im Datenschutzrecht geltenden Grundsatz der Erforderlichkeit darstellen würde, wurde zunächst ein Gesetzentwurf erstellt, der eine entsprechende Regelung enthielt. Aufgrund des Einlenkens von Seiten der Ärzte wurde von dem Vorhaben dieser Gesetzesänderung jedoch wieder Abstand genommen.

Obwohl ich darauf hinwies, dass vor Beginn des elektronischen Verfahrens „Einladungswesen“ ein fachspezifisches Datenschutzkonzept erstellt werden müsse, wurde am 1. Dezember 2007 mit dem Einladungswesen begonnen, ohne dass diesem gesetzlichen Erfordernis nachgekommen worden war. Immerhin wurde Ende November 2007 eine Verfahrensbeschreibung übersandt; die von Gesetzes wegen notwendige Festlegung der technisch-organisatorischen Maßnahmen steht hingegen noch aus.

12.3.2 Meldung von Kindern, die im Haushalt von Substitutionspatienten leben

Im Januar 2007 wies mich eine Bremer Arztpraxis darauf hin, die Kassenärztliche Vereinigung Bremen (KVHB) habe alle substituierenden Ärztinnen und Ärzte in Bremen schriftlich dazu aufgefordert mitzuteilen, bei welchen ihrer Substitutionspatienten Kinder im Haushalt leben. Kurz darauf meldete sich auch die KVHB und bat um eine datenschutzrechtliche Einschätzung zu der von ihr zwei Wochen zuvor versandten Aufforderung. Ich kritisierte die verkehrte Vorgehensweise. Weiterhin gab ich zu bedenken, dass Ärztinnen und Ärzte der ärztlichen Schweigepflicht unterliegen und es für eine entsprechende Meldung keine gesetzliche Grundlage gebe. Diese sei daher nur aufgrund einer freiwilligen Einwilligungserklärung der betroffenen Patienten zulässig. Zudem gehe aus dem von der KVHB erstellten Meldeformular nicht deutlich hervor, welche Daten von den Ärzten übermittelt werden sollen. Die Datenübermittlung sollte sich auf die Daten beschränken, die benötigt werden, um das betreffende Kind zu identifizieren. Eine Übermittlung von Daten der Eltern sei dafür nicht erforderlich und daher verzichtbar. Daneben wies ich darauf hin, dass es nicht zu den gesetzlichen Aufgaben der KVHB gehört, bei der Feststellung von Kindeswohlgefährdungen mitzuwirken und ich daher eine entsprechende Datenerhebung durch die KVHB für unzulässig halte.

Ich konnte schließlich erreichen, dass die Meldung sich auf die Daten Name, Vorname und Geburtsdatum des Kindes beschränkt und nur mit Einwilligung des Betroffenen direkt vom substituierenden Arzt ohne Zwischenschaltung der KVHB an das Amt für Soziale Dienste, Abteilung Junge Menschen und Familie, erfolgt. Zudem unterstützte ich die KVHB bei der Erstellung eines Einwilligungsformulars, welches den Anforderungen des § 4 a BDSG genügt.

12.3.3 Betreuung drogenabhängiger Schwangerer und Eltern

Im März 2007 wurde mir vom Gesundheitsressort des Senators für Arbeit, Frauen, Gesundheit, Jugend und Soziales ein Konzept für einen Kontrakt „Leitlinien und Verfahrensregeln für die Beratung und Betreuung drogenabhängiger Schwangerer, Mütter und Eltern durch die Bremer Drogenhilfe“ zur Kenntnis gegeben. Mit diesem vom Gesundheitsamt und zwei Bremer Drogenhilfeeinrichtungen zu unterzeichnenden Kontrakt sollte sichergestellt werden, dass ein Kind nur bei einer drogenabhängigen Mutter verbleiben kann, wenn diese sich mit dem Ziel der Überwindung der Drogenabhängigkeit intensiv betreuen lässt und dabei kooperativ zeigt. Die betroffenen drogenabhängigen Schwangeren und Eltern sollten unter anderem verpflichtet werden, eine Schweigepflichtentbindungserklärung abzugeben, um einen Datenaustausch zwischen den an der Betreuung beteiligten Einrichtungen zu ermöglichen. Die Mitarbeiter von Drogenhilfeeinrichtungen sollten aber auch gegen den Willen der Betroffenen zur Meldung an das Amt für soziale Dienste verpflichtet werden.

Ich wies darauf hin, dass eine Schweigepflichtentbindungserklärung nur wirksam sei, wenn sie auf der freien Entscheidung der Betroffenen beruht. Daher könnten drogenabhängige Schwangere oder Eltern nicht dazu verpflichtet werden, eine entsprechende Erklärung abzugeben. Daraufhin wurde der Passus mit der Verpflichtung zur Schweigepflichtentbindungserklärung aus der Vereinbarung gestrichen. Im Übrigen wies ich darauf hin, dass die Ärzte und Drogenberatungsstellen einer besonderen Schweigepflicht unterliegen, deren Durchbrechung durch eine Rechtsgrundlage gedeckt sein müsse. Nach Unterzeichnung des Kontraktes erkundigte ich mich bei den beiden beteiligten Drogenhilfeeinrichtungen, aufgrund welcher Sachverhalte nach Unterzeichnung des Kontraktes bisher Meldungen an das Amt für Soziale Dienste erfolgt seien, um zu überprüfen, ob dies mit der geltenden Rechtslage in Einklang steht. Eine Rückmeldung der Einrichtungen, die eine entsprechende Bewertung ermöglicht, steht bisher noch aus.

Zur konkreten Ausgestaltung des oben genannten Kontraktes wurde mir dann im November der Entwurf einer Fachlichen Weisung „Umgang mit Kindern substituierter bzw. drogenabhängiger Mütter/Väter bzw. Eltern“ vom Amt für Soziale Dienste zur Stellungnahme übersandt. Dieser Entwurf traf konkrete Regelungen hinsichtlich einer Kooperation und damit eines umfassenden Datenaustauschs zwischen den Familienhebammen des Gesundheitsamtes, den substituierenden niedergelassenen Ärzten, Frauen-, Kinder-, Jugend- und Hausärzten, Drogenhilfeeinrichtungen, den im Rahmen der Betreuung drogenabhängiger Eltern tätigen Trägern, Krankenhäusern, Schulen, dem Amt für Soziale Dienste, Nachbarn und sozialen Netzwerken von drogenabhängigen Eltern. Die in dem Entwurf vorgesehenen Datenübermittlungen bedürfen zunächst noch einer vertieften rechtlichen Überprüfung durch die Fachabteilungen der senatorischen Dienststellen, die noch nicht abgeschlossen ist.

12.3.4 Aufforderung an Krankenhäuser zur Datenübermittlung an das Amt für Jugend und Familie

Im Juli 2007 meldete sich der Diözesendatenschutzbeauftragte der Katholischen Kirche bei mir und setzte mich darüber in Kenntnis, dass das Amt für Jugend und Familie (AfJuF) zwei Krankenhäuser in Bremerhaven per E-Mail auf die Möglichkeit der Information des AfJuF bei Kindeswohlgefährdungen durch Alkohol oder Drogen hingewiesen hatte. Der Jugendhilfeplaner des AfJuF führte in seiner E-Mail unter anderem aus, dass im Rahmen der gesetzlichen Garantenpflichten das AfJuF über das Bekanntwerden der Möglichkeit einer Kindeswohlgefährdung nach Abschätzung des Gefährdungspotentials informiert werden sollte. Der E-Mail war ein Formular beigefügt, das benutzt werden sollte, wenn ein Kind/Jugendlicher wegen übermäßigem Alkohol- oder Drogengenuss im Krankenhaus medizinisch betreut werden muss. Nach Auffassung des Jugendamtes liege in diesen Fällen eine Kindeswohlgefährdung vor. Die Einzelfallentscheidung sei aber natürlich im Krankenhaus vor Ort zu treffen. Das für die Meldung beigefügte Formular, das Felder für die Eintragung von Name, Geburtsdatum, Sorge- bzw. Erziehungsberechtigter, Anschrift, Telefon und Anlass der Meldung enthält, ist lediglich mit den E-Mailadressen der im AfJuF zuständigen Ansprechpartner versehen.

Ich wandte mich daraufhin an das AfJuF und teilte mit, dass es keine Garantenpflicht für einen behandelnden Arzt zur Meldung an das Jugendamt bei Bekanntwerden oder der Möglichkeit von Kindeswohlgefährdungen gebe. Dem stehe die ärztliche Schweigepflicht entgegen, deren Verletzung in § 203 StGB sogar strafbewehrt sei. Eine Befugnis zur Mitteilung von Kindeswohlgefährdungen an Dritte bestehe nur entweder aufgrund einer Einwilligung des betroffenen Patienten bzw. seines gesetzlichen Vertreters oder unter den Voraussetzungen des rechtfertigenden Notstands nach § 34 StGB. Tatbestandsvoraussetzung des § 34 StGB sei eine gegenwärtige, nicht anders abwendbare Gefahr für ein Rechtsgut (z. B. Leib oder Leben). Das Vorliegen dieses Tatbestandsmerkmals sei allein aufgrund eines (evtl. einmaligen) übermäßigen Alkohol- und Drogengenusses eines Kindes oder Jugendlichen jedoch wohl in der Regel nicht erfüllt. Für die Beurteilung, ob eine gegenwärtige Gefahr für das Kind bzw. den Jugendlichen vorliegt, sei eine Einbeziehung aller weiteren bekannten Umstände des Falles notwendig. Nur wenn durch Andauern der Gefahrensituation der Eintritt eines Schadens für das Kind in Zukunft wahrscheinlich sei, liege eine gegenwärtige Gefahr vor.

Weiter wies ich darauf hin, dass die Ausgestaltung des für die Meldung beigefügten Formulars zu einer Datenübermittlung per E-Mail verleiten könne. Eine Übermittlung von personenbezogenen Daten unverschlüsselt per E-Mail genügte jedoch nicht den besonderen Anforderungen des Datenschutzes gemäß § 7 Abs. 4 Bremisches Datenschutzgesetz (BremDSG) und § 9 Bundesdatenschutzgesetz (BDSG). Ich äußerte die Bitte, entsprechende „Angebote“ zukünftig im Vorfeld mit mir abzustimmen.

Daraufhin versicherte das Amt, aufgrund meiner Intervention die Krankenhäuser um eine Meldung auf dem Postwege gebeten zu haben. Hinsichtlich meiner fachlichen Einschätzung, ob und wann eine Kindeswohlgefährdung durch Alkohol oder Drogen vorliege, würden für das Amt weder Tatbestandsvoraussetzungen des § 34 StGB noch meine Ansichten über (evtl. einmaligen) übermäßigen Alkohol- und Drogengenuss eine Rolle spielen. Diese Antwort lässt befürchten, dass es mir trotz meiner ausführlichen Erläuterung wohl leider nicht gelungen ist, dem zuständigen

Sachbearbeiter des Amtes die Verpflichtung eines Arztes zur Wahrung seiner Schweigepflicht zu verdeutlichen.

Erfreulicherweise kann man dies den beiden betroffenen Krankenhäusern nicht vorwerfen, von denen eines sich unverzüglich an den zuständigen (kirchlichen) Datenschutzbeauftragten wandte und das andere sich nach Erhalt einer ausführlichen Information bei mir herzlich bedankte und versicherte, sich an die gesetzlichen Bestimmungen zu halten.

12.3.5 Meldung der Krankenkasse bei Verdacht auf Kindeswohlgefährdung

Im April 2007 rief mich der Datenschutzbeauftragte einer Bremer Krankenkasse an und fragte, ob für die Krankenkasse bei Verdacht auf Kindeswohlgefährdung eine Befugnis bzw. Verpflichtung zur Datenübermittlung an das Jugendamt bestehe. Ich teilte ihm mit, dass es für eine entsprechende Datenübermittlung im SGB V, den bereichsspezifisch geregelten Datenübermittlungsvorschriften für Krankenkassen, keine Rechtsgrundlage gebe und wies zudem darauf hin, dass die Informationslage der Krankenkassen in der Regel nicht hinreichend präzise ist, um eine solche Feststellung zu treffen. Vielmehr verfügt der behandelnde Arzt schon aufgrund seiner eigenen Wahrnehmungen bei der Behandlung des Kindes über wesentlich mehr Informationen als die Krankenkasse, die diese Informationen lediglich in Form von ICD-Schlüsseln erreicht. Es liegt in der Verantwortung des behandelnden Arztes, bei Hinweisen auf eine gegenwärtige Kindeswohlgefährdung die zuständigen Stellen in Kenntnis zu setzen. Deshalb sollte die Entscheidung des Arztes zur Wahrung bzw. zum Bruch seiner Schweigepflicht grundsätzlich akzeptiert werden. Gegen eine entsprechende Rückfrage seitens der Kassen beim Arzt bestehen hingegen keine Bedenken. Im Übrigen wäre in den Fällen, in denen die Krankenkasse die Daten von einem Arzt erhalten hat, die Übermittlung von Sozialdaten auch nur unter den Voraussetzungen zulässig, unter denen der Arzt selbst übermittlungsbefugt wäre. Der behandelnde Arzt unterliegt der ärztlichen Schweigepflicht. Eine Befugnis zur Mitteilung von Kindeswohlgefährdungen an Dritte besteht für den behandelnden Arzt nur entweder aufgrund einer Einwilligung des betroffenen Patienten oder unter den Voraussetzungen des rechtfertigenden Notstandes nach § 34 StGB. Demnach wäre auch die Krankenkasse nur unter diesen Voraussetzungen zur Datenübermittlung an das Jugendamt befugt. Neben der Einholung einer Einwilligung der gesetzlichen Vertreter des betroffenen Kindes käme ein Tätigwerden nach § 34 StGB in Betracht. Voraussetzung dafür ist eine gegenwärtige, nicht anders abwendbare Gefahr für ein Rechtsgut (z. B. Leib oder Leben). Ob diese tatsächlich vorliegt, kann nur bei genauer Kenntnis aller Umstände beurteilt werden. Über dieses Wissen verfügen die Kassen in der Regel nicht.

12.3.6 Hinweis auf mögliche Kindeswohlgefährdung landet bei in Verdacht geratener Familie

Im Oktober meldete sich eine Bürgerin bei mir, die per E-Mail einen anonymen Hinweis auf eine mögliche Kindeswohlgefährdung beim Sozialzentrum Nord des Amtes für Soziale Dienste gegeben hatte. Sie teilte mit, kurz darauf von der betroffenen Familie eine beleidigende E-Mail erhalten zu haben, in der ihr vorgeworfen werde, sich in dieser Sache an die Behörde gewandt zu haben. Zudem habe sie eine E-Mail ohne Inhalt vom Sozialzentrum erhalten. Sie bat um Aufklärung der Frage, wie die betroffene Familie an ihre E-Mail-Adresse gekommen sei und weshalb sie eine Nachricht ohne Text vom Sozialzentrum erhalten hatte.

Meine Nachfrage ergab, dass die Leiterin des Sozialzentrums eine E-Mail an die Bürgerin geschickt hatte, um zu testen, ob deren Adresse tatsächlich existiere. Die E-Mail mit der anonymen Meldung sei von einer Service-Mitarbeiterin „versehentlich“ an alle 105 im Sozialzentrum beschäftigten Mitarbeiter weitergeleitet worden, obwohl sie eigentlich nur an drei zuständige Mitarbeiter hätte weitergeleitet werden dürfen. Daher konnte nach Aussage der Sozialzentrumsleiterin nicht mehr festgestellt werden, durch wen die E-Mail-Adresse an die betroffene Familie weitergegeben worden sei. Es wurde jedoch versichert, dass die Anonymität von Beschwerdeführern grundsätzlich gewahrt werde.

Ich bewertete die Weiterleitung der E-Mail an alle Mitarbeiter des Sozialzentrums als gravierenden Verstoß gegen die Verpflichtung zur Wahrung des Sozialgeheimnisses nach § 35 Abs. 1 Satz 2 SGB I, die den Sozialleistungsträger verpflichtet, auch innerhalb der Behörde sicherzustellen, dass Sozialdaten nur Befugten zugänglich sind bzw. an diese weitergegeben werden und bat um Erläuterung der nach § 78 a SGB X erforderlichen technischen und organisatorischen Maßnahmen, die eine Einhaltung des Sozialgeheimnisses sicherstellen sollen. Auch der Test, ob es sich bei der E-Mail-Adresse um eine „echte“ Adresse handele, erschließt sich mir nicht, da schließlich nur von einer „echten“ Adresse E-Mails versandt werden können. Auch hatte das Amt für Soziale Dienste selbst behauptet, die Anonymität solcher Meldungen zu gewährleisten.

Die Leiterin des Sozialzentrums teilte mit, dass es sich um eine einmalige Verfehlung einer Mitarbeiterin im Service gehandelt habe und dass daraufhin alle Mitarbeiterinnen und Mitarbeiter im Service von ihr noch einmal schriftlich auf die Einhaltung der vorhandenen Regelungen hingewiesen worden seien. Zudem habe sie nicht erkannt, dass die Bürgerin hier anonym bleiben wollte, da sie ihre Meldung per E-Mail abgegeben habe.

13. Bildung und Wissenschaft

13.1 Erst die Daten, dann das Abiturzeugnis

Mir ist ein Schreiben des Schulamtes Bremerhaven an die Schulleitungen der Gymnasialen Oberstufen zur Evaluation der Einführung zentraler Prüfungen vorgelegt worden, in dem behauptet wird, ich sei bei der wissenschaftlichen Begleitung der Einführung zentraler Abiturprüfungen in Bremen und Bremerhaven beteiligt worden. Da ich erst auf diesem Wege von der Evaluation erfuhr, habe ich dem Schulamt gegenüber meine Verwunderung zum Ausdruck gebracht und um Stellungnahme gebeten.

Der von den Schülerinnen und Schüler auszufüllende Fragebogen enthielt unter anderem Fragen über die Eltern, ohne dass diese die Möglichkeit erhalten, in die Beantwortung einzuwilligen. Im Rahmen einer Nacherhebung solle die Aushändigung des Abiturzeugnisses von der Rückgabe des ausgefüllten Fragebogens abhängig gemacht werden. Ich musste das Schulamt auf § 13 Abs. 2 Bremisches Schuldatenschutzgesetz (BremSchulDSG) hinweisen, wonach die Teilnahme an der Fragebogenaktion nur auf freiwilliger Basis zulässig ist.

Des Weiteren ist mir zu dieser Untersuchung ein Lehrerfragebogen vorgelegt worden, in dem entgegen der Hinweise auf die Anonymität eine Vielzahl von Angaben zur Person abgefragt werden, die einen Rückschluss auf einzelne Lehrkräfte ermöglichen. Die Anonymität wäre damit offensichtlich nicht gewährleistet worden. Es sind jedoch nur solche Angaben zur Person zulässig, die keinen Rückschluss auf einzelne Lehrkräfte ermöglicht.

Nach meinen Erfahrungen aus anderen Erhebungen werden im Übrigen dann keine ehrlichen und demzufolge nicht brauchbaren Antworten gegeben, etwa zu Fragen der Zufriedenheit oder zu sonstigen persönlichen Befindlichkeiten - gerade im Zusammenhang mit dem Arbeitsplatz -, wenn die Anonymität nicht gewährleistet ist.

Das Schulamt hat erklärt, verantwortlich für das Vorhaben sei die senatorische Dienststelle Bildung und Wissenschaft. Nach Rücksprache mit der senatorischen Behörde ist mir zugesagt worden, meine Anforderungen zu berücksichtigen und die Erhebung erst nach deren Umsetzung durchzuführen.

13.2 Bundeszentrale Datei über Schüler und Lehrer

Die Kultusministerkonferenz (KMK) beabsichtigt, die bisherige Schulstatistik auf Individualdaten umzustellen und hierbei einen bundeseinheitlichen Datensatz mit einer Vielzahl von Daten zu jedem einzelnen Schüler zentral zu speichern (vgl. 29. JB, Ziff. 13.2 und Ziff. 19.7). Den dabei mangelnden Datenschutz hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder kritisiert. Im Laufe des Berichtsjahres hat die Kommission für Statistik der KMK ein überarbeitetes „Konzept für die länderübergreifende Weiterverarbeitung und Nutzung von Individualdaten“ vorgelegt. Auch dieses Konzept beantwortet weiterhin grundsätzliche datenschutzrechtliche Fragen nicht.

So fehlt eine klare Darlegung, ob nicht anstelle der mit dem vorgelegten Konzept verbundenen Datenvollerhebungen und Weiterverarbeitungen, die zukünftig absehbar einen erheblichen technisch-organisatorischen, finanziellen und personellen Aufwand zur Folge haben werden, Untersuchungen im Bildungsbereich, die sich auf fundierte wissenschaftliche Analysen einzelner Problemfelder beschränken, denselben Zweck erfüllen. Insbesondere ist als Basis für die Prüfung der Verhältnismäßigkeit der Maßnahme nachvollziehbar darzulegen, welche konkreten Ziele und Zwecke der Schülerstatistik als amtliche Statistik ausschließlich durch eine Totalerhebung erreichbar sein sollen sowie, ob die Maßnahme verhältnismäßig ist.

Ungeachtet der ausstehenden Klärung dieser Grundfrage bedeutet der sich abzeichnende Verzicht auf den Schulidentifikator - und damit auch den Klassenidentifikator - einen datenschutzrechtlichen Fortschritt. Eine datenschutzgerechte Bildung eines Pseudonyms erscheint grundsätzlich möglich, die hierfür erforderlichen Maßnahmen wurden aber bisher noch nicht getroffen. Datenverarbeitungen im Zuge der Schulstatistik in dem beabsichtigten Umfang für noch zu benennende Zwecke wären zudem nur auf dem Weg der Einführung einer amtlichen Statistik und ihrer Erhebungsinstrumentarien zulässig, die gesetzlich zu regeln wäre.

Inzwischen haben zwei Sitzungen der Kommission für Statistik der KMK stattgefunden, an denen auch Vertreter von Landesbeauftragten für den Datenschutz teilgenommen haben. Es besteht nach wie vor Dissens, insbesondere hinsichtlich der zentralen Frage der Totalerhebungen zur Durchführung von Bildungsverlaufsuntersuchungen. Darüber hinaus besteht noch erheblicher Klärungsbedarf insbesondere zu folgenden Gesichtspunkten:

- die Einzelheiten zu temporären Zusammenfassungen der Daten für länderübergreifende Auswertungen,
- die Festlegung, welche Daten übermittelt werden sollen,
- die Bewertung der Erforderlichkeit der im Zentraldatensatz enthaltenen Daten und
- die Festlegung der Erhebungs- und Hilfsmerkmale (z. B. beim Merkmal „Migrationshintergrund“).

13.3 Zusammenarbeit zwischen Schule, Justiz, Polizei sowie Jugend- und Sozialbehörden

Die Senatorin für Bildung und Wissenschaft hat mir den Entwurf einer Vereinbarung über die Zusammenarbeit zwischen den oben genannten Stellen mit der Bitte um Stellungnahme zugeleitet. Ziel und Inhalt der Vereinbarung sind die Verbesserung der ressortübergreifendenden Zusammenarbeit im Bereich der Schulen sowie eine systematische und aufeinander abgestimmte Zusammenarbeit bei Verhaltensauffälligkeiten von Schülerinnen und Schülern. Der Entwurf regelt Datenübermittlungen der Schule an die Polizei, Informationsbefugnisse der Polizei, Informationen an die Jugendhilfe durch die Schule und Informationen durch und an die Justiz (Staatsanwaltschaft und Gerichte).

Die Vereinbarung soll die Schulleitung bei Vorliegen der in der Vereinbarung genannten Straftaten zur Einschaltung der Polizei verpflichten, wenn diese in unmittelbarem Zusammenhang mit der Schule stehen und gegen oder durch Schülerinnen und Schüler begangen worden sind oder eine solche Straftat bevorsteht.

Ich habe die senatorische Dienststelle darauf hingewiesen, dass als Grundlage jeder Datenübermittlung von Schulen an die genannten Stellen die neue Regelung des § 8 Bremisches Schuldatenschutzgesetz (BremSchulDSG) zu beachten ist (vgl. 29. JB, Ziff. 13.1). Insbesondere bedeutet dies, dass nach § 8 Abs. 1 Satz 2 BremSchulDSG bei jeder Datenübermittlung an eine dieser Stellen der Erziehungs- und Bildungsauftrag der Schule sowie das Vertrauensverhältnis zwischen den Schülerinnen und Schülern und der Schule zu berücksichtigen ist und die Datenübermittlung nur durch die Schulleitung erfolgen darf. Darüber hinaus sind bei Datenübermittlungen der Jugendhilfe, Polizei und Justiz an die Schulen die jeweiligen bereichsspezifischen gesetzlichen Regelungen, wie Sozialgesetzbuch VIII, Bremisches Polizeigesetz, die für die Strafverfolgung geltenden Mitteilungen in Strafsachen (MiStra) und Jugendgerichtsgesetz anzuwenden. Insoweit darf keine der in dem Entwurf enthaltenen Regelungen zur Datenübermittlung den gesetzlich vorgegebenen Rahmen nicht überschreiten.

Des Weiteren sah der Entwurf vor, dass die Polizei Informationen über Personen, Taten oder Sicherheitslagen, welche für den schulischen Bereich zur Abwehr einer Gefahr oder zur Erfüllung der Aufgaben der Polizei erforderlich sind, der Schulleitung mitteilen darf. Außerdem sei das Jugendamt unverzüglich zu unterrichten, wenn schon während der polizeilichen Ermittlung erkennbar wird, dass eine erhebliche Notlage vorliegt oder die Abwehr einer schwerwiegenden Beeinträchtigung der Rechte eines Schulkindes notwendig ist, ferner, wenn Leistungen der Jugendhilfe in Frage kommen.

Hinsichtlich der Informationen an die Jugendhilfe durch die Schule habe ich angemerkt, dass im Rahmen der Beteiligung der Jugendhilfe nur die für die Erfüllung der Aufgaben der Jugendhilfe nach dem Sozialgesetzbuch VIII erforderlichen Daten übermittelt werden dürfen. Das Gleiche gilt auch für die Teilnahme der Jugendhilfe an Fallkonferenzen der Schulen. Anlage dieser Vereinbarung soll ein bereits eingesetzter Leitfaden zur Anwendung des § 47 a Bremisches Schulgesetz (BremSchulG) sein, zu dem ich ebenfalls ausführlich Stellung genommen habe.

Es stellt sicherlich eine akzeptable Vorgehensweise dar, wenn die Verwaltung sich zunächst zusammensetzt und überlegt, welche Informationen jeweils für die eigene Arbeit hilfreich sein können.

In einem zweiten Schritt muss dann allerdings geprüft werden, ob diese Überlegungen auch mit den vorhandenen gesetzlichen Regelungen in Einklang stehen. Es war daher klar, dass die jetzt auf den Weg gebrachte Zusammenarbeitsvereinbarung sich an den gesetzlich vorhandenen Regelungen ausrichten musste. Eine Verwaltungsvereinbarung kann keine gesetzliche Grundlage schaffen, sondern vorhandene nur interpretieren. Den Schulleitungen und Lehrern kann daher nur das aufgegeben werden, was im vorgesehenen gesetzlichen Rahmen zulässig ist. Dies war auch die Grundlage für meine Beratung der Verwaltungsvereinbarung. Unabhängig davon muss natürlich eine solche Zusammenarbeitsvereinbarung mit Leben gefüllt werden. Nach meiner Auffassung bietet der mir jetzt vorliegende Entwurf genügend Spielraum, im Rahmen der Ermessensausübung der betroffenen Stellen zu wesentlich verbesserten Formen der Zusammenarbeit zu gelangen.

14. Umwelt, Bau, Verkehr und Europa

14.1 Online-Anbindung der örtlichen Fahrerlaubnisbehörden an das ZFER

Bei der Einführung des Zentrale Fahrerlaubnisregisters (ZFER) beim Kraftfahrt-Bundesamt (KBA) im Jahr 1999 hatte der Gesetzgeber die Abschaffung der örtlichen Fahrerlaubnisregister vorgesehen. Das Straßenverkehrsgesetz sieht dazu den Stichtag 31. Dezember 2006 vor. Eine weitergehende Regelung ist noch nicht getroffen worden. Fahrerlaubnisbehörden löschen seitdem in großem Umfang ihre Datensätze, sobald diese im zentralen Register eingestellt worden sind.

Nach dem derzeitigen Stand einer Online-Anbindung der Fahrerlaubnisbehörden an das Zentrale Fahrerlaubnisregister des KBA fehlen jedoch Vorkehrungen zur Datensicherheit, die gewährleisten, dass die dort eingegebenen Fahrerlaubnisdaten integer, authentisch, revisionsfähig und transparent verarbeitet werden.

Die rechtliche und technische Ausgestaltung berücksichtigt nicht hinreichend, dass die Daten zunehmend ausschließlich beim KBA vorgehalten werden. Dies wirft verschiedene Probleme auf, z. B. hinsichtlich

- der Anforderungen an den Online-Dialogbetrieb (lesender und schreibender Zugriff der Erlaubnisbehörden),
- der Beweissicherheit einzelner Verfahrensschritte auch über lange Zeit und
- der datenschutzrechtlichen Verantwortlichkeiten.

Angesichts des Umfangs der personenbezogenen Daten, die zukünftig ausschließlich zentral und mit Schreibbefugnis für alle Fahrerlaubnisbehörden verarbeitet werden sollen, ist es dringend erforderlich, die Rechtsverbindlichkeit dieser Informationen sowohl für die Betroffenen als auch für die Behörden dauerhaft sicherzustellen.

Die hierzu in einem Gutachten des Arbeitskreises Verkehr der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Einzelnen aufgezeigten rechtlichen und technischen Probleme und Defizite in der Datensicherheit gefährden die Rechtsverbindlichkeit und die erforderliche Beweissicherheit der ausschließlich elektronisch gespeicherten personenbezogenen Daten der Fahrerlaubnisinhaberinnen und –inhaber. Für Letztere steht als technisches Verfahren mit langfristiger Überprüfbarkeit die qualifizierte elektronische Signatur mit Anbieterakkreditierung der Sachbearbeitenden zur Verfügung. Für die Gewährleistung der sicheren Übertragung der Fahrerlaubnisdaten sind die Prinzipien des Standards OSCI-Transport 1.2 zu berücksichtigen.

Daher ist die Bundesregierung aufgefordert, die notwendigen Änderungen im Straßenverkehrsgesetz und der Fahrerlaubnisverordnung in die Wege zu leiten und dafür zu sorgen, dass die gesetzlichen Regelungen den tatsächlichen und zukünftig angestrebten Verhältnissen angepasst und rechtsverbindliche Festlegungen für die Datensicherheit und insbesondere für die Beweissicherheit getroffen werden.

Ich habe den Senator für Umwelt, Bau, Verkehr und Europa darüber unterrichtet und ihn gebeten, sich für die Umsetzung der notwendigen rechtlichen Anpassung einzusetzen.

14.2 Zugriff der Bauordnungsbehörde auf das Melderegister

Der Senator für Umwelt, Bau, Verkehr und Europa hat mir den Entwurf zur Änderung der Bremischen Meldedatenübermittlungsverordnung (BremMeldDÜV) vorgelegt. Der Abruf aus dem Melderegister soll zum Zweck der Überprüfung unzulässiger Wohnnutzung in Parzellengebieten erweitert werden. Begründet wurde dies mit der Bereinigung von Kleingartengebieten bezogen auf illegale Nutzung und Schwarzbautätigkeit sowie Gefahrenabwehr (ordnungsgemäße Entsorgung von Grundstücken, Einhaltung des vorbeugenden Brandschutzes und Standsicherheit). Monatlich würden aus den vorstehenden Gründen bislang 800 Einzelabfragen in schriftlicher Form an die Meldebehörde erforderlich, von denen im Jahr 200 Anfragen eilbedürftig seien. Ich habe u. a. vorgeschlagen, in dem Entwurf die Zwecke konkret zu benennen und den Umfang der zur Übermittlung zugelassenen Daten auf die für den Verwendungszweck regelmäßig benötigten Angaben zu begrenzen. Gegen den daraufhin überarbeiteten Entwurf bestehen keine Bedenken.

14.3 Bericht aus dem Arbeitskreis Verkehr

Im Berichtszeitraum hat der AK Verkehr der Konferenz der Datenschutzbeauftragten des Bundes und der Länder einmal getagt und dabei schwerpunktmäßig die Themen Online-Anbindung der Fahrerlaubnisbehörden an das Zentrale Fahrerlaubnisregister (ZFER) des Kraftfahrtbundesamtes (KBA), Verbunddateien zum Verfahrensmanagement von Großraum- und Schwertransporten, personenbezogene Datenverarbeitung im Lagezentrum See (maritimes Sicherheitszentrum) sowie Novellierung des Seeaufgabengesetzes, Videobeobachtung für Verkehrsleitsysteme und Fernübertragung von Videoaufnahmen aus öffentlichen Verkehrsmitteln an die Leitstelle des Verkehrsunternehmens behandelt.

15. Finanzen

15.1 Einführung einer lebenslangen Identifikationsnummer für jeden Bürger

Zum 1. Juli 2007 ist auf Bundesebene die steuerliche Identifikationsnummer eingeführt worden. Jeder in Deutschland gemeldete Bürger erhielt im Laufe des Jahres 2007 eine vom Bundeszentralamt für Steuern verwaltete, eindeutige Identifikationsnummer zugeteilt. Die Identifikationsnummer wird künftig mit der Geburt vergeben und bleibt bis 20 Jahre über den Tod des Betroffenen hinaus gespeichert.

Für die Zuteilung der Identifikationsnummer mussten die etwa 5.500 Meldebehörden in Deutschland bis Ende September 2007 dem Bundeszentralamt für Steuern die Stammdaten der in ihrem Melderegister registrierten Einwohner sowie künftig alle Neuzugänge und Änderungen übermitteln. Weitgehend unbemerkt von der Öffentlichkeit ist damit ein bundeseinheitliches zentrales Melderegister errichtet, das bislang stets abgelehnt worden ist.

Die Abgabenordnung sieht vor, dass die Identifikationsnummer nur zur Erfüllung der gesetzlichen Aufgaben der Finanzbehörden verwendet werden darf. Die Datenschutzbehörden haben jedoch in der Vergangenheit immer wieder die Erfahrung gemacht, dass der Gesetzgeber zunächst eine strenge Zweckbindung der Daten vorgesehen hat und im nachhinein schwach geworden ist und eine Reihe weiterer Verwendungsmöglichkeiten zugelassen hat. Die Abgabenordnung lässt bereits jetzt die Verwendung der Identifikationsnummer für andere Zwecke zu, wenn eine Rechtsvorschrift dies ausdrücklich erlaubt. Damit besteht praktisch eine Einladung an den Gesetzgeber.

Bestätigt wurden meine Befürchtungen, als ich im Herbst von dem geplanten Vorhaben „openELSTER“ erfuhr, bei dem die im Rahmen von ELSTER zur Authentifizierung aufgebaute Trustcenter-Infrastruktur anderen öffentlichen Stellen für E-Government-Anwendungen zur Verfügung gestellt werden sollte. Nach dem Konzept sollten die Zertifikate unter Verwendung der Steueridentifikationsnummer auf ihre Gültigkeit hin geprüft werden. Hiergegen habe ich mich gegenüber der Senatorin für Finanzen gewandt, wie andere Datenschutzbeauftragte. Daraufhin wurde von dem Entwicklerland und dem Bundesministerium für Finanzen mitgeteilt, dass es zunächst um eine Interessenanfrage bei den Ländern gehe und das Konzept vor einer eventuellen Umsetzung später zwingend in diesem Punkt überarbeitet werde.

Eine eindeutige Personenkennziffer, die Verwechslungen auch bei Umzügen oder Namensänderungen ausschließt, wird auch in der Privatwirtschaft, bei Auskunfteien oder Adresshändlern auf großes Interesse stoßen, und so ist zu befürchten, dass sie die zukünftige Basis von Persönlichkeitsprofilen bilden wird.

15.2 Entscheidung des Bundesverfassungsgerichts zum Kontostammdatenabruf

Das Bundesverfassungsgericht hat mit Beschluss vom 13. Juni 2007 (1 BvR 1550/03, 1 BvR 2357/04, 1 BvR 603/05) entschieden, dass ein Teil der Regelungen zum Abruf von Kontostammdaten in der Abgabenordnung gegen das Gebot der Normenklarheit verstößt und daher verfassungswidrig ist. Der Kreis der abfrageberechtigten Behörden und die Aufgaben, denen solche Kontostammdatenabrufe dienen sollen, sind nicht hinreichend bestimmt. Zugleich hat das Verfassungsgericht jedoch die weiteren Rechtsgrundlagen für Kontostammdatenabrufe durch Finanzbehörden gebilligt.

15.3 Bericht aus dem Arbeitskreis Steuerverwaltung

Der AK Steuerverwaltung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder befasste sich im Berichtsjahr u. a. mit folgenden Themen: verschiedene automatisierte Verfahren der Steuerverwaltung, wie KONSENS (Koordinierte Neue Software Entwicklung der Steuerverwaltung) mit seinen Bausteinen LUNA (LänderUmfassende NamensAbfrage), Xpider und ZEUGE (ZStV- / BZR-ErmittlungsUnterstützung auf der Grundlage von EOSS [Evolutionär Orientierte SteuerSoftware]). Daneben wurde die Koordinierungsrunde zur Abgabenordnung im Hinblick auf die Einführung eines Auskunftsanspruchs in die Abgabenordnung und § 88 a Abgabenordnung, der nur eine unzureichend allgemeine Rechtsgrundlage darstellt angesichts der Vielzahl bundesweit eingesetzter automatisierter Programme, thematisiert. Weitere Themen waren das automatisierte Verfahren ZAUBER, das Steueränderungsgesetz 2007, Auskunftsverweigerungsrechte nach § 102 Abgabenordnung, Telearbeit in der Steuerverwaltung und die Anwendbarkeit von Informationsfreiheitsgesetzen im Besteuerungsverfahren.

16. Wirtschaft und Häfen

16.1 Verfahrensbeschreibung „Datei Hafensicherheit“

Im Sommer 2006 habe ich gegenüber der Polizei Bremen Stellung genommen zu der Verfahrensbeschreibung der Datei Hafensicherheit, mit der die Beteiligung der Polizei an der Zuverlässigkeitsüberprüfung nach dem Hafensicherheitsgesetz beschrieben wird. Die Verfahrensbeschreibung war veraltet, enthielt falsche Begrifflichkeiten und Rechtsgrundlagen, sah die Verarbeitung einer Reihe von Daten vor, die das Hafensicherheitsgesetz nicht zuließ und statuierte nicht zutreffende Löschfristen. Sie enthielt auch keine hinreichenden Angaben zu den technisch-organisatorischen Maßnahmen zur Datensicherheit des verwendeten Polizeirechners.

Nach einer Besichtigung vor Ort im September 2006 und der ersten Überarbeitung der Verfahrensbeschreibung wies ich im Oktober 2006 auf ausstehende Angaben bei den technisch-organisatorischen Maßnahmen hin und erinnerte im Januar 2007 an die Erledigung. Auf erneute Erinnerung Anfang Mai 2007 erhielt ich Mitte Mai eine angepasste Verfahrensbeschreibung, die aufgrund der zwischenzeitlichen Novellierung des Hafensicherheitsgesetzes Ende April 2007 jedoch bereits wieder unzutreffend war. So hatten sich die Rechtsgrundlagen, der Zweck der Zuverlässigkeitsüberprüfung und der Umfang der zu verarbeitenden Daten verändert. Offen blieben immer noch einige technisch-organisatorische Fragen. Zudem machte ich darauf aufmerksam, dass die Verfahrensbeschreibung nach § 8 BremDSG, anders als das Datenschutzkonzept nach § 7 Abs. 2 BremDSG, öffentlich einsehbar ist, da die Polizei Bremen die Verfahrensbeschreibung nunmehr zur Verschlusssache erklärt hatte.

Im Oktober 2007 erhielt ich eine erneut überarbeitete Fassung, die nunmehr eine Trennung in einen öffentlichen und einen nicht öffentlichen Teil vollzog. Da weiterhin einige Fragen zu technisch-organisatorischen Maßnahmen offen geblieben waren, bat ich im November 2007 erneut um Stellungnahme, die Ende Dezember 2007 erfolgte. Ich hoffe, dass das Verfahren nunmehr datenschutzkonform betrieben werden kann.

16.2 Neues Bremisches Hafensicherheitsgesetz

Mitte Januar 2007 wurde mir vom Senator für Wirtschaft und Häfen der Entwurf des neuen Hafensicherheitsgesetzes zur Stellungnahme übersandt. Neben der Anpassung an europarechtliche Rechtsvorschriften sollte das Gesetz auch in der Vergangenheit aufgetretene Probleme in der Praxis behandeln.

In meiner Stellungnahme wies ich Ende Januar 2007 neben redaktionellen Änderungsvorschlägen darauf hin, dass die Befugnis der Polizei, im Rahmen der Kontrolle des grenzüberschreitenden Verkehrs die Aushändigung aller hierfür erforderlichen Papiere verlangen zu können, sich mit der Pflicht des Schiffsführers überschneidet, der Polizei die zur grenzpolizeilichen Aufgabenwahrnehmung erforderlichen Daten zu übermitteln. Zudem sah der Entwurf vor, dass Aufgaben der Zuverlässigkeitsüberprüfung auf das Hansestadt Bremische Hafenamt als nachgeordnete Behörde übertragen werden können. Hiergegen habe ich aufgrund der Komplexität und Sicherheitsrelevanz des Verfahrens Bedenken geäußert. Ferner sollten im Rahmen des Zuverlässigkeitsüberprüfungsverfahrens die beteiligten Sicherheitsbehörden zur eindeutigen Identifizierung u. a. auch den Wohnort und die Staatsangehörigkeit des Betroffenen erfahren. Das hielt ich nicht für erforderlich, zumal in der Vergangenheit keine Probleme aufgetreten waren. Zudem knüpfte die Nachberichtspflicht, d. h. die Pflicht, nachträglich erlangte Erkenntnisse über eine überprüfte Person mitzuteilen, an Informationen und nicht an Tatsachen an. Die Nachberichtspflicht droht dadurch auszuufern, da „weiche“ Daten wie Meinungsbekundungen übermittelt werden, ohne dass mangels Überprüfbarkeit dieser Informationen ein Sicherheitsgewinn erzielt wird.

Die Überschneidung der Polizeibefugnisse wurde in der Gesetzesbegründung klargestellt wie auch der Hinweis, dass eine Kompetenzübertragung der Zuverlässigkeitsüberprüfungen auf eine nachgeordnete Behörde nicht stattfindet. Die letzten beiden Punkte konnten, obwohl die praktischen Probleme gesehen wurden, nicht gegenüber dem Senator für Inneres und Sport durchgesetzt werden, der auf die parallele Regelung im Bereich der Luftsicherheit hinwies und darauf, dass das Landesamt für Verfassungsschutz fast nie Tatsachen übermittele und seine Nachberichtspflicht dann leer liefe. Allerdings wurde klargestellt, dass die Unzuverlässigkeit nicht aufgrund einer Empfehlung des Landesamtes für Verfassungsschutz ausgesprochen werde, die sich auf Informationen stütze, die es nicht mitteilen könne. Am 30. April 2007 wurde das neue Bremische Hafensicherheitsgesetz verabschiedet (Brem.GBl. S. 307).

17. Bremerhaven

17.1 Themen aus Bremerhaven

An dieser Stelle werden alle Ziffern aufgeführt, die sich mit Themen aus Bremerhaven beschäftigen. Sie finden sich unter Ziff. 9.10 (Entwurf eines Bundesmeldegesetzes), Ziff. 9.13 (Fingerabdruckdaten in Reisepässen), Ziff. 9.17 (Übermittlung von Meldedaten an politische Parteien vor den Wahlen), Ziff. 9.18 (Eingaben in Bezug auf politische Parteien und Wahlinitiativen im Zusammenhang mit den Wahlen), Ziff. 10.1 (Prüfung von Gerichtsvollziehern), Ziff. 11.2 (Prüfung im Bereich Krankengeld der AOK Bremen/Bremerhaven), Ziff. 12.1 (Datenschutz in der BAgIS und der ARGE Job Center Bremerhaven), Ziff. 12.3.4 (Aufforderung an Krankenhäuser zur Datenübermittlung an das Amt für Jugend und Familie), Ziff. 13.1 (Erst die Daten, dann das Abiturzeugnis), Ziff. 17.2 (Datenschutz im Petitionsverfahren) und Ziff. 20.3 (Öffentlichkeitsarbeit, Vorträge, Fortbildungsangebote und Kooperationen).

17.2 Datenschutz im Petitionsverfahren

Ich hatte darüber berichtet, dass es heftigen Streit zwischen zwei Nachbarn in Bremerhaven gegeben hatte, weil der eine sich in ein Verwaltungsverfahren des anderen mittels einer Petition eingemischt hatte und Nachbarn oder Dritte die sehr persönlich und subjektiv gehaltene Petition - wahrscheinlich im Rahmen eines (anwaltlichen) Akteneinsichtsverfahrens (Genaues ließ sich nicht mehr feststellen) - zur Kenntnis bekommen hatten. Das Petitionsschreiben oder die Vorwürfe daraus waren vom Petitionsausschuss der Verwaltung zur Stellungnahme zugeleitet worden. Jedenfalls landeten Kopien des Petitionsschreibens mit üblen Beschimpfungen im Briefkasten des Petenten. Nach Vortrag der Sachlage und Empfehlungen aus meinem Hause hat der Magistrat Bremerhaven prompt reagiert und in seiner Mitteilung 7/07 im Februar 2007 die folgende Regelung getroffen:

„Unterlagen aus Petitionsverfahren bedürfen einer besonders vertraulichen Behandlung. Sie enthalten häufig Erklärungen des Petenten, mit denen er sich vertrauensvoll an die Stadtverordnetenversammlung gewandt hat und die keiner unbefugten Stelle oder Person zugänglich gemacht werden dürfen. Insbesondere muss der mit der Regelung in § 1 Abs. 5 des Ortsgesetzes getroffenen Bestimmung, dass niemand wegen der Ausübung seiner Rechte nach diesem Gesetz benachteiligt werden darf, auch im weiteren Verwaltungsverfahren Rechnung getragen werden.

Wegen ihrer besonderen Schutzwürdigkeit und um sicherzustellen, dass Unterlagen oder Daten aus Petitionsverfahren nicht unzulässig weitergegeben werden, empfiehlt es sich, diese Unterlagen bzw. Kopien getrennt von anderen aus dem betreffenden Verwaltungsvorgang stammenden Schriftstücken aufzubewahren.

Darüber hinaus sind generell in allen Fällen einer Akteneinsicht, Aktenauskunft, Aktenüberlassung oder beim Fertigen von Kopien aus diesem Anlass gewisse Regularien einzuhalten. Vor der Gewährung der Akteneinsicht muss die Identität des Einsichtbegehrenden und sein Einsichtrecht zweifelsfrei festgestellt werden. Vor der Überlassung der Akte an einen Rechtsanwalt hat dieser eine Vollmacht vorzulegen. Haben mehrere Bürger ein Recht auf Akteneinsicht in dieselbe Akte, ist sicherzustellen, dass eine vorhergehende Einsichtnahme durch eine andere Person dem Einsichtbegehrenden nicht bekannt wird. Die Gewährung einer Akteneinsicht muss überprüfbar sein. Sie ist daher, ggf. mit der Vollmacht des Rechtsanwalts, zu dokumentieren.“

Damit sind für die Zukunft klare Regelungen geschaffen, es lässt sich damit wenigstens feststellen, wer Einsicht in eine Verwaltungsakte genommen hat.

18. Datenschutz auf internationaler Ebene

18.1 Verarbeitung von Flugpassagierdaten

Übermittlung von Flugpassagierdaten in die USA: Am 1. August 2007 ist das neue Abkommen zur Übermittlung von Flugpassagierdaten in die USA in Kraft getreten. Hierdurch sollte das am 31. Juli 2007 abgelaufene Interimsabkommen abgelöst werden (vgl. 26. JB, Ziff. 17.3 und 27. JB, Ziff. 15.2). Nach dem nun geltenden Abkommen soll von einem Pull- auf ein Pushsystem übergegangen werden. Es ist aber noch nicht geklärt, ob überhaupt und unter welchen Bedingungen dafür gesorgt wird, dass diese neue Art der Übermittlung funktioniert. Weiterhin sollen künftig 19 statt 34 Datensätze über Flugpassagiere erhoben und in die USA übermittelt werden. Diese Absenkung stellt allerdings nur einen Sieg auf dem Papier dar, weil sie aus einer Zusammenfassung verschiedener Datenelemente resultiert.

Im Einzelnen werden folgende Datenfelder übermittelt:

1. ein Code zur Identifizierung des PNR (Passagiernamensregister / Passenger Name Record),
2. Datum der Reservierung und der Ausstellung des Flugscheins,
3. geplante Abflugdaten,
4. Name(n) des Passagiers,
5. Informationen über Vielflieger- und Bonusprogramme und gewährte Rabatte,
6. andere Namen im PNR, einschließlich Zahl der Reisenden im PNR,
7. alle verfügbaren Kontaktinformationen (einschließlich Auftraggeberinformationen),
8. alle verfügbaren Zahlungs-/Abrechnungsinformationen (ohne weitere Transaktionsdetails für eine Kreditkarte oder ein Konto, die nicht mit der die Reise betreffenden Transaktion verknüpft sind),
9. Reiseverlauf für den jeweiligen PNR,
10. Reisebüro/Sachbearbeiter des Reisebüros, bei dem das Ticket gebucht wurde,
11. Code-Sharing-Informationen (gemeinsames Anbieten von Flügen durch mehrere Fluggesellschaften; ein einzelner Flug erhält hierbei verschiedene Flugnummern),
12. Informationen über Aufspaltung/Teilung einer Buchung.
13. Reisestatus des Fluggastes (einschließlich Bestätigungen und Eincheckstatus),
14. Information über das Ticket, einschließlich Flugscheinnummer, Angabe, ob Flugschein für einfachen Flug, sowie Automatic Ticket Fare Quote (automatische Tarifabfrage),
15. sämtliche Informationen zum Gepäck,
16. Sitzplatzinformationen, einschließlich Sitzplatznummer,
17. allgemeine Bemerkungen einschließlich Informationen zur besonderen Behandlung des Passagiers (OSI – Other Service Information, SSI – Special Service Information, SSR – Special Service Requests; enthalten Information z.B. für Passagiere mit Behinderungen, besonderen Essenswünschen o.Ä.),

18. etwaig erfasste APIS-Daten (Advance Passenger Information System – beinhaltet Daten zu Namen, Adressen, Passnummer sowie, falls vorhanden, biometrische Daten aus den Ausweisdokumenten),

19. alle Änderungen der unter den Nummern 1 bis 18 aufgeführten Daten.

Darüber hinaus enthält das Abkommen viele weitere datenschutzrechtliche Verschlechterungen. Das US-Heimatschutzministerium darf jetzt in Ausnahmefällen sensible Daten verwenden, was durch das frühere Abkommen ausgeschlossen war. Die anschließende Weitergabe an andere US-amerikanische oder ausländische Behörden ist erleichtert worden und unterliegt nicht mehr denselben Datenschutzgarantien. Zudem werden die Daten künftig 15 statt bisher dreieinhalb Jahre in den USA vorgehalten. Das Abkommen wird von der Artikel 29-Datenschutzgruppe als deutlicher Rückschritt kritisiert (vgl. hierzu http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp138_de.pdf).

Verwendung von Flugpassagierdaten innerhalb der Europäischen Union: Auch auf europäischer Ebene gibt es Bestrebungen, Flugpassagierdaten für Strafverfolgungszwecke zu nutzen. Dieses geht aus dem Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen hervor. Ziel des Rahmenbeschlusses ist es, Daten über Fluggäste, welche die europäischen Grenzen überqueren, in nationalen Datenbanken zu speichern, untereinander auszutauschen, auszuwerten und für Zwecke der Verhütung und Bekämpfung terroristischer Straftaten und von Straftaten der organisierten Kriminalität zu nutzen. Die Fluggesellschaften sollen verpflichtet werden, zu jedem Fluggast insgesamt 18 Datenelemente, bei unbegleiteten Minderjährigen zusätzlich 6 Datenelemente, zu übermitteln. Es ist geplant, die Datenelemente aktiv fünf und danach in einer „ruhenden“ Datenbank mindestens weitere acht Jahre zu speichern. Die Umsetzung des geplanten Rahmenbeschlusses wäre weder mit dem im europäischen Grundrecht auf Datenschutz (Art. 8 der EU-Grundrechte-Charta) noch mit dem vom Grundgesetz garantierten Recht auf informationelle Selbstbestimmung vereinbar. Es handelt sich hierbei um eine anlassunabhängige Vorratsspeicherung von Verkehrsdaten. Eine solche ist unverhältnismäßig und begegnet verfassungsrechtlichen Bedenken, weil sie die Speicherung von Daten aller Fluggäste ohne jeden Verdacht anordnet. Im Übrigen sind die zu erhebenden Daten von zweifelhafter Eignung.

18.2 Internationale Konferenz der Beauftragten für den Datenschutz

Ende September 2007 tagte in Montreal (Kanada) die 29. Internationale Konferenz der Beauftragten für Datenschutz und die Privatsphäre. Hier wurden folgende Entschließungen gefasst:

- Resolution über den dringenden Bedarf an globalen Standards zum Schutz von Passagierdaten, die von Regierungsstellen zu Justizvollzugs- und Grenzschutzzwecken herangezogen werden,
- Resolution über die Entwicklung internationaler Standards für die Anwendung und eine
- Resolution über den Einsatz neuer und bestehender Technologien sowie über die internationale Zusammenarbeit der Datenschutzbeauftragten.

19. Datenschutz in der Privatwirtschaft

19.1 Zu den Sitzungen der obersten Datenschutzaufsichtsbehörden

Um länderübergreifend in der Bundesrepublik aber auch EU-weit einen möglichst einheitlichen Datenschutzstandard zu gewährleisten, bedarf es der Absprache unter den Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich. An den Sitzungen der obersten Aufsichtsbehörden – jeweils eine im Frühjahr und im Herbst – nehme ich regelmäßig teil. Um wirtschaftliche Belastungen der Unternehmen zu vermeiden, bin ich daran interessiert, den datenschutzrechtlichen Regelungen Geltung zu verschaffen und dabei möglichst keine zusätzlichen Arbeitsaufwände zu erzeugen. Eine über die Grenzen einheitliche Haltung der Datenschutzaufsichtsbehörden gegenüber der Wirtschaft ist auch deshalb wichtig, um gleiche wirtschaftliche Rahmenbedingungen zu erzeugen und so Wettbewerbsverzerrungen zu vermeiden. Das gilt natürlich für alle Wirtschaftszweige, im besonderem Maße aber für die, deren Geschäftsfeld ausschließlich im Bereich der Datenverarbeitung liegt.

Einige der nachfolgend aufgeführten Themen werden im weiteren Verlauf des Berichtes näher erläutert. Im Bereich der Kreditwirtschaft bestand Anlass, sich mit Themen wie Kreditscoring/Basel II, dem Verkauf von Darlehen an Unternehmer ins Ausland oder der Datenverarbeitung bei SWIFT zu befassen. Im Übrigen bestehen ständige Themen im Bereich der Telekommunikation, Tele- und Mediendienste, der Versicherungswirtschaft, dem Adress- und Versandhandel wie im Bereich des Arbeitnehmerdatenschutzes. Der Patientendatenschutz in Kooperationspraxen war ebenso Thema wie Mandantenschutz in Rechtsanwaltskanzleien, aber auch Einzelthemen wie Bonus- und Rabattkarten, Digi-Foto-Maker oder Mahnung per Computer waren Gegenstand der Beratungen. Auch bei der Gesetzgebungsberatung, z. B. der Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes (hier mit Regelungen für Auskunfteien und das Scoring) und dem Entwurf des Bundesdatenschutzauditgesetzes fand ein Meinungsaustausch statt. Soweit zu den einzelnen Themen Beschlüsse gefasst wurden, sind diese auf der Homepage des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter www.bfdi.bund.de abrufbar.

19.2 Kreditwirtschaft

19.2.1 Unzureichende Protokollierung von Beschäftigtenzugriffen bei einem Kreditinstitut

Ich erhielt mehrere Beschwerden unzulässiger Datenabrufe von Kundenkonten durch Beschäftigte eines Kreditinstituts.

Ich bemühte ich mich um Aufklärung des Sachverhaltes und bat das Kreditinstitut zunächst um Darstellung der von ihm verwirklichten Protokollierung der Zugriffe der Mitarbeiterinnen und Mitarbeiter. Da die Darstellung verschiedene Fragen aufwarf, besuchte ich im November 2007 schließlich das Kreditinstitut und informierte mich vor Ort über die Protokollierung.

Dabei stellte sich heraus, dass das Kreditinstitut ein im Kern seit 1971 bestehendes Datenverarbeitungssystem betreibt, bei dem die Zugriffe zwar elektronisch protokolliert, jedoch tagesaktuell auf Mikrofiche verfilmt und dem betrieblichen Datenschutzbeauftragten zur Verfügung gestellt werden. Aufgrund einer seinerzeit geschlossenen Vereinbarung mit dem Betriebsrat, um Leistungs- und Verhaltenskontrollen der Mitarbeiter auszuschließen, war es dem betrieblichen Datenschutzbeauftragten daher nicht möglich, die Mikrofiche z. B. nach den Zugriffen bestimmter Mitarbeiter oder Zeiten zu überprüfen. Auch gestaltete sich die Überprüfung der Kontrolle ohne elektronische Unterstützung durch Sichtung der Mikrofiche als äußerst mühsam, da täglich etwa 250.000 Zugriffe bremenweit protokolliert wurden.

Diese Form der Protokollierung steht nicht im Einklang mit den technisch-organisatorischen Anforderungen, die das Bundesdatenschutzgesetz für Protokollierungen aufstellt. Ich habe das Kreditinstitut, das sich bereits im Prozess der Migration auf ein neues Programm befand, hierüber in Kenntnis gesetzt und verschiedene Anforderungen an die künftige Protokollierung gestellt.

Da sich im Nachgang der Prüfung ergab, dass die verfilmten Protokolldaten zur Wiederherstellung im Katastrophenfall doch auch elektronisch vorgehalten werden, habe ich die Sicherung der Protokolldaten und eine Auswertung verlangt, um den Verdacht eines missbräuchlichen Zugriffs zu beseitigen. Dieser Vorgang ist noch nicht abgeschlossen.

19.2.2 SWIFT

Alle Auslandsüberweisungen werden weltweit über SWIFT abgewickelt. Die datenschutzrechtliche Problematik der auch auf Drittländer außerhalb der EU verteilten Datenverarbeitung von SWIFT habe ich im letzen Bericht dargestellt (vgl. 29. JB, Ziff. 18.3). Im Oktober 2007 hat SWIFT die geplante Veränderung ihrer IT-Infrastruktur bekannt gegeben. Der Art. 29-Gruppe hatte SWIFT vorher noch einige nähere Erläuterungen gegeben.

Danach soll der Systemumbau bis Ende 2009 erfolgen. Die DV soll dann auf drei Server verteilt sein. In der Schweiz wird der „globale“ Serverstehen, d. h., dort werden alle Daten gespiegelt. Außerdem wird es weiterhin einen Server in den USA und einen in Europa (Niederlande) geben. Der Server in den USA wird alle Daten der „Transatlantic Zone“ speichern; auf dem europäischen Server werden alle Überweisungsdaten der „European Zone“ gespeichert werden. Zur „European Zone“ gehören alle Staaten des europäischen Wirtschaftsraums und die Schweiz. Zur „Transatlantic Zone“ gehören die USA. Alle anderen Staaten können wählen, zu welcher Zone sie gehören wollen, d. h., Länder wie Japan oder die Türkei können selbst entscheiden, ob sie zur europäischen oder transatlantischen Zone gehören wollen. Diese Frage soll von den entsprechenden nationalen Mitgliedsgruppen von SWIFT und nicht von den Regierungen entschieden werden; die entsprechenden Entscheidungen der Mitgliedsstaaten sollen öffentlich gemacht werden.

Das bedeutet: Zur Zeit werden Überweisungen innerhalb der Staaten des europäischen Wirtschaftsraumes und der Schweiz nur auf dem Server in den Niederlanden gespeichert und in der Schweiz gespiegelt. Bei Überweisungen in die USA wird eine Speicherung in den USA erfolgen.

19.3 Auskunfteien

19.3.1 Handels- und Wirtschaftsauskunfteien

Im Berichtsjahr erhielt ich Eingaben, die sich gegen die Datenverarbeitung der Auskunfteien richteten. Hier einige Beispiele:

Ein Betroffener beklagte sich bei mir, dass Daten zu einer gegen ihn gerichteten Forderung in den Auskunfteidatenbestand der für seinen Wohnort zuständigen Geschäftsstelle einer Handels- und Wirtschaftsauskunftei aufgenommen worden seien. Kenntnis von der Forderung habe er erstmalig durch das an ihn von dieser Auskunftei im Rahmen der Inkassotätigkeit des Unternehmens übersandten Mahnschreibens erhalten, dem er auch die Informationen zur Übernahme seiner Daten in den Auskunfteidatenbestand entnommen hatte.

Auch Auskunfteien dürfen nur richtige Daten verarbeiten. Ist die gegen einen Schuldner erhobene Forderung berechtigt und wurde sie termingerecht beglichen, so sind Aufnahme und Übermittlung von Angaben zu Auskunfteizwecken, nach denen der Betroffene seinen Zahlungsverpflichtungen nicht nachkommt oder es sich bei ihm um einen säumigen Schuldner handelt, nicht zulässig. Die Aufnahme und Übermittlung einer noch nicht titulierten und nicht beglichenen Forderung setzen voraus, dass der Betroffene von der bevorstehenden Nutzung für Auskunfteizwecke rechtzeitig informiert wird. Rechtzeitig ist die Unterrichtung nur, wenn dem Betroffenen noch die Möglichkeit verbleibt, in zumutbarer Weise ggf. ein berechtigtes Bestreiten der Forderung voranzubringen oder zu begleichen. Im vorliegenden Fall hätte der Betroffene keine Möglichkeit gehabt, die Berechtigung der Forderung zu überprüfen und dieser zu entsprechen bzw. sie zu bestreiten. Die Aufnahme und Übermittlung der Daten zu Auskunfteizwecken wäre daher unzulässig gewesen.

Meine Nachforschungen bei der Auskunftei ergaben, dass entgegen des Wortlauts des Mahnschreibens eine Aufnahme der den Petenten betreffenden Inkassodaten in den Auskunfteidatenbestand bislang nicht erfolgt war. Dies wurde mir auch von der für den Wohnort zuständigen Geschäftsstelle bestätigt. Die Auskunftei bedauerte, dass es durch missverständliche Formulierungen in dem Mahnschreiben zu einem falschen Eindruck gekommen war und sagte zu, die in dem Schreiben kritisierten Textpassagen künftig nicht mehr zu verwenden.

In einem anderen die Tätigkeit dieser Auskunftei betreffenden Fall beklagte sich ein Betroffener, dass seinem Anspruch auf Auskunft nach § 34 BDSG nicht entsprochen werde. Seine Bitte um Mitteilung, woher die Auskunftei seine Daten habe, werde nicht erfüllt. Erst durch mein Tätigwerden gelang es, den gesetzlichen Anspruch des Betroffenen durchzusetzen.

19.3.2 Wohnungsunternehmen als Vertragspartner der SCHUFA

Bereits 2003/2004 wurde kontrovers diskutiert, inwieweit Auskunfteien und Warndateien Auskünfte über Mietinteressenten an Vermieter vor Eingehung eines Mietverhältnisses erteilen dürfen. Zur Teilnahme von Wohnungsunternehmen am Auskunftsverfahren der SCHUFA und anderer Auskunfteien, aber auch zu Auskünften an einzelne Vermieter haben die obersten Datenschutzaufsichtsbehörden im November 2004 sich auf allgemeine Grundsätze verständigt.

Aus der Sicht des Datenschutzes sind auf branchenspezifische Daten beschränkte Auskunftssysteme vorzuziehen, bei denen die Daten gesicherte Rückschlüsse auf Mietausfallrisiken zulassen. Dies entspricht auch Vorstellungen, die derzeit im Deutschen Bundestag diskutiert werden.

Eine uneingeschränkte Auskunft über bei branchenübergreifenden Auskunfteien gespeicherte Daten an potentielle Vermieter ist dagegen unzulässig. an Vermieter zu übermitteln, nicht gerechtfertigt ist. Die kompletten Negativdaten etwa, wie sie anderen B-Partnern zur Verfügung gestellt werden, dürfen an Vermieter nicht weitergegeben werden.

Bei der Prüfung, in welchem Umfang nach § 29 Bundesdatenschutzgesetz an potentielle Vermieter personenbezogene Daten übermittelt werden dürfen, sind die schutzwürdigen Belange der Mietinteressenten im Hinblick auf die Bedeutung der Wohnung für die Lebensgestaltung in besonderer Weise zu berücksichtigen. Auskünfte über Eintragungen im Schuldnerverzeichnis sind stets zulässig.

Die obersten Datenschutzaufsichtsbehörden haben auch Zweifel an der Zulässigkeit einer Beauskunftung auf Grund einer Einwilligung. Entsprechendes gilt auch für das Verlangen gegenüber dem Mietinteressenten auf Vorlage einer Selbstauskunft. Unter den Aufsichtsbehörden ist unstreitig, dass diese rechtliche Beurteilung fortgilt.

19.3.3 Prüfung einer Auskunftei mit Mieterdaten in Bremen

In den Geschäftsräumen einer Mieterauskunftei fand die vorgenannte Prüfung statt. Prüfungsschwerpunkte waren die Datenerhebung bei Dritten, Datenspeicherung, Datenübermittlung an Dritte und die Gewährleistung der Betroffenenrechte.

Datenerhebung bei Dritten und Datenspeicherung: Die Mieterauskunftei erhält Daten aus unterschiedlichen Quellen, z. B. von Vermietern. Diese melden Daten über Verstöße gegen erhebliche mietvertragliche Verpflichtungen durch Mieter sowie eine Vielzahl anderer Daten an die Mieterdatenbank, z. B. Kaution vertragsgemäß gezahlt, Mietrückstand, Mängelanzeige rechtzeitig, Tierhaltung.

Neben der Mieterdatenbank hält die Mieterauskunftei eine sog. Bonitätsdatenbank vor. Diese enthält den branchenübergreifenden Datenbestand einer in Baden-Württemberg ansässigen Auskunftei entsprechend deren Katalog über Auskunftsmerkmale und Hinweis-Meldungen. Außerdem werden Daten von anderen Auskunfteien branchenübergreifend in diese Bonitätsdatenbank eingestellt. Die von der Auskunftei in Baden-Württemberg bezogenen Daten sind nach dortiger Kategorisierung, die nicht auf die Bonitätsprüfung durch Vermieter bezogen ist, in „weiche“ (z. B. Inkasso-Mahnverfahren eingeleitet), „mittlere“ (Mahnbescheid) und „harte“ (z. B. Eröffnung des Insolvenzverfahrens) Negativmerkmale unterteilt.

Die Erhebung von Daten durch die Mieterauskunftei, die zusätzlich zu den Angaben über erhebliche Mietvertragsverstöße und den sog. harten Negativmerkmalen eingemeldet werden, ist aus folgenden Gründen nicht zulässig:

Bei der Frage, welche personenbezogenen Mieterdaten ein Vermieter zur Bonitätsprüfung benötigt und demzufolge erhoben bzw. in die Mieterdatenbank eingegeben werden dürfen, ist zwischen den nachstehenden Rechtsgütern des Vermieters und des Mietinteressenten angemessen abzuwägen.

Die berechtigten Interessen des Vermieters bestehen insbesondere darin, das Mietausfallrisiko zu vermindern. Insoweit ist einer Prüfung anzuerkennen, ob der Mietinteressent in der Lage ist, die Miete zu bezahlen. Bedeutsam ist hierbei auch, dass der Vermieter sog. schwarze Schafe und sog. Mietnomaden unter den Mietinteressenten erkennen möchte, um mögliche Risiken auch im Lichte des Mietvertrags abzuschätzen.

Die schutzwürdigen Interessen des Mietinteressenten bestehen aufgrund der existentiellen Bedeutung einer Wohnung als Mittelpunkt des privaten Lebensbereiches und seiner grundrechtlichen Schutzposition aus Art. 2, 13, 14 Grundgesetz (GG) und den Vorschriften des Mietrechts nach §§ 535 ff. Bürgerliches Gesetzbuch (BGB). Erfahrungsgemäß unterscheidet sich das Zahlungsverhalten im allgemeinen Geschäftsverkehr erheblich von dem Verhalten im Mietverhältnis. Gleichwohl muss hier ein Betroffener damit rechnen, als Mieter abgelehnt zu werden, wenn der Vermieter von der Auskunftei über das Vorliegen eines Vollstreckungsbescheides informiert wird, der aus einer nicht bezahlten Rechnung, z. B. aus einem Kaufvertrag, resultiert.

Die Bonitätsprüfung und die daraus resultierende Datenerhebung durch den Vermieter bei Auskunfteien müssen sich an der spezifischen Situation des anzubahnenden Mietverhältnisses orientieren. Vermieter können zur Bonitätsprüfung die Vorlage von Verdienstbescheinigungen etc. durch den Mietinteressenten nach § 4 Abs. 2 Satz. 1 i. V. m. § 28 Abs. 1 Satz 1 Nr. 1 BDSG

verlangen. Außerdem befinden sich Vermieter gegenüber dem Mietinteressenten im Vorteil, z. B. durch die Mietkaution, das Vermieterpfandrecht und ggf. in die Zahlungspflicht tretende Sozialbehörden, die bei Zahlungsunfähigkeit die Mietzahlung übernehmen. Daher ist die Erheblichkeitsschwelle bei mietspezifischen oder sonstigen mieterrelevanten Negativdaten hoch anzusetzen. Demzufolge benötigt ein Vermieter nicht sämtliche bei einer allgemeinen Auskunftei gespeicherten Daten zur Bonitätsprüfung. Nach Abwägung beider Rechtsgüter ist nur die Erhebung bzw. Einmeldung sog. harter Daten und keiner sog. Bagatelldaten bzw. „weicher“ und „mittlerer“ Daten zulässig.

Erforderliche Angaben von Auskunfteien zur Prüfung der Bonität von Mietern: Unter Beachtung dieser Bewertung sind folgende Angaben für die Prüfung der Bonität von Mietern durch die Erhebung bei einer Auskunftei erforderlich und zulässig:

- Daten aus öffentlichen Schuldnerverzeichnissen (eidesstattliche Versicherung, Haftanordnung und Insolvenz),
- rechtskräftige Titel zu Zahlungsverzug im Mietbereich,
- rechtskräftige Urteile zur fristlosen Kündung eines Mietvertrages wegen Zahlungsverzug oder bei sonstiger Verletzung des Mietvertrages,
- rechtskräftiges Räumungsurteil wegen fristloser Kündigung,
- Daten über sog. Mietnomaden, wenn innerhalb der ersten drei Monate zwei Monatsmieten nicht gezahlt wurden und eine Strafanzeige wegen Betrugs nach § 263 Strafgesetzbuch (StGB) durch den Vermieter erstattet wurde.

Außerdem sind aus den vorgenannten Gründen zur Einhaltung des § 29 BDSG bzgl. der Mieterdatenbank die im Datenkatalog eingeteilten Daten und die Einmeldungen aus anderen Auskunfteien in die Bonitätsdatenbank entsprechend zu markieren und festzulegen, so dass nur sog. harte Daten in die Mieterdatenbank aufzunehmen sind.

Datenübermittlung an Dritte: Soweit anfragende Vermieter die in der Mieterdatenbank enthaltenen Angaben nicht für ausreichend halten, greifen sie auf die Bonitätsdatenbank der Mieterauskunftei zu. Dadurch erhalten sie neben den Angaben über Mietvertragsverstöße und den „harten“ alle über den Mietinteressenten gespeicherten sonstigen „weichen“ und „mittleren“ Daten; und zwar branchenübergreifend. Umgekehrt können Kunden, die keine Vermieter sind, auch auf die Mieterdatenbank zugreifen.

Infolge des Zugriffs auf beide Datenbanken durch die Vermieter und die übrigen Kunden erfolgt keine notwendige Trennung und Markierung der Datensätze für die Bonitätsprüfung von Mietinteressenten und für die Bonitätsprüfung außerhalb von Mietvertragsverhältnissen. Die Vermieter dürfen für den Abschluss von Mietverträgen Nur Zugriff auf die hierfür benötigten Daten haben, die in der Vermieterdatenbank gespeichert sind. Die übrigen Kunden dürfen nur auf die Bonitätsdatenbank zugreifen.

Es bedarf daher einer klaren technischen und organisatorischen Trennung der Mieterdatenbank von der allgemeinen Bonitätsdatenbank, einschließlich der daraus folgenden Sperrung des jeweils unzulässigen Zugriffs auf die andere Datenbank. Zur Gewährleistung dieser Trennung sind die erforderlichen Maßnahmen nach § 9 BDSG zu treffen.

Gewährleistung der Betroffenenrechte: Bei der erstmaligen Übermittlung wird der Betroffene von der Mieterauskunftei in einem Formschreiben darüber unterrichtet, dass an einen Vermieter mit einem berechtigten Interesse Daten zu seiner Person übermittelt wurden, weil er im Begriff ist, mit ihm ggf. einen Mietvertrag abzuschließen. Über den Datensatz kann sich der Betroffene bei der Mieterauskunftei informieren.

Das verwendete Formschreiben entsprach nicht den Anforderungen des § 33 Abs. 1 Satz 2 BDSG. Eine Anpassung des Schreibens war insbesondere im Hinblick auf die Art der übermittelten Daten erforderlich.

Es besteht die Möglichkeit, Selbstauskünfte einzuholen. Diese enthalten alle über den Betroffenen gespeicherten Daten. Im Hinblick auf die Berichtigung unrichtiger Daten wurden die Betroffenen bislang an die Auskunftei verwiesen, bei der die Daten erhoben wurden. Zur Sperrung von Daten teilte die Mieterauskunftei mit, die Daten würden - so sie bestritten worden sind - bis zu einer Klärung nicht mehr übermittelt.

Die Mieterauskunftei wurde darauf hingewiesen, dass der Berichtigungsanspruch nach § 35 BDSG in vollem Umfang auch ihr gegenüber besteht und demzufolge der Geltendmachung derartiger Ansprüche zu entsprechen ist.

19.3.4 Änderung des Bundesdatenschutzgesetzes (BDSG) – Auskunfteien und Scoring

Der Handel mit bonitätsgeprüften Informationen hat sich zu einem lukrativen Markt entwickelt, da detaillierte Informationen zur wirtschaftlichen Situation einzelner Personen wertvoll sind. Während zunächst nur Waren und Kredite vergebende Unternehmen an diesen bei Auskunfteien gespeicherten Daten interessiert waren, hat sich dieser Kreis mittlerweile erheblich ausgeweitet. Vor allem auf Dienstleistungsunternehmen jedweder Art, teilweise sogar unabhängig davon, ob sie bei einem konkreten Geschäft ein wirtschaftliches Risiko tragen.

Je mehr Abnehmer die Auskunfteien für ihre Daten haben, desto umfangreicher werden ihre eigenen Dateien, da die Abnehmer zugleich Datenlieferanten sind. Die Empfänger von Daten verpflichten sich nämlich, Daten über den Geschäftsverlauf oder über Unregelmäßigkeiten beim Geschäftsverlauf den Auskunfteien mitzuteilen. So besteht seit Jahren der Trend bei Auskunfteien, ihre Geschäftsfelder zur Erhöhung des wirtschaftlichen Ertrags auszuweiten.

Dem Datenschutz wird dabei nicht immer die ausreichende Aufmerksamkeit entgegengebracht, weil die Auskunfteien in keinerlei geschäftlichen oder vertraglichen Beziehungen mit den Betroffenen stehen, deren Daten gespeichert und an Dritte übermittelt werden. Ein wachsendes Netz verschiedener Auskunftssysteme und branchenübergreifender Zentraldateien ermöglicht eine Profilbildung, bei der das Verhalten eines bestimmten Menschen ohne dessen Wissen und Wollen abgebildet wird und ihn so für Dritte berechenbar macht.

Angesichts dieser Tendenzen sind die sehr allgemein gehaltenen gesetzlichen Regelungen zum Datenschutz der Bürgerinnen und Bürger im Auskunfteienbereich nicht mehr ausreichend und daher ergänzungsbedürftig. Aus der Praxis der Datenschutzaufsichtsbehörden heraus haben sich Überlegungen ergeben, Regelungen zur Datenverarbeitung zu präzisieren und deren Transparenz für die Betroffenen zu verbessern.

Folgende Grundsätze sind bei Auskunftssystemen zu beachten:

- Verbot der Mitteilung über die Tatsache einer Datensperre an Dritte,
- Wegfall der Einschränkung des Auskunftsrechts unter allgemeinem Verweis auf das Geschäftsgeheimnis,
- Möglichkeit zur Selbstauskunft einmal im Jahr kostenfrei,
- Unterrichtung des Betroffenen vor einer Einmeldung durch die einmeldende Stelle zur Wahrung seiner Rechte auf u. a. Berichtigung und Sperrung seiner Daten,
- Erweiterung der Benachrichtigungspflicht auf Art und Herkunft der Daten gegenüber dem Betroffenen, die bei Dritten nur für Zwecke der Beauskunftung erhoben und hierfür kurzfristig bei der Auskunftei gespeichert werden,
- Benachrichtigung auch durch Auskunfteien bereits bei der erstmaligen Speicherung von Daten zum Betroffenen und nicht erst bei der erstmaligen Übermittlung,
- klare Anforderungen für ein ausreichendes Bestreiten der Richtigkeit der gespeicherten Daten durch den Betroffenen,

- Verkürzung der Löschungsfrist auf drei Jahre,
- Erweiterung des Bußgeldtatbestandskatalogs auf Verstöße gegen dieVorschriften zum Auskunftsrecht.

Darüber hinaus sind besondere Regelungen für branchenspezifische Auskunftssysteme erforderlich, hier insbesondere die Trennung und Beschränkung auf vertragsrelevante Daten bei Speicherung und Auskunftserteilung.

Beim Scoring, unabhängig davon, ob dies von einer Auskunftei oder von einem Unternehmen selbst durchgeführt wird, sind folgende Grundsätze zu beachten:

- klare Transparenz des Scorings für den Betroffenen durch entsprechende Unterrichtung durch den Scorewertschaffenden und den Scorewertverwendenden,
- Offenlegung der Merkmale und deren Gewichtung,
- Scoringverbot für vertragserfüllungsfremde Daten wie z. B. Wohnumfeld, ethnische Herkunft,
- Nutzbarkeit nur von vertragsrelevanten Daten für das Scoring.

Inzwischen hat das Bundesministerium des Innern (BMI) hierzu einen Entwurf zur Änderung der Regelungen des BDSG vorgelegt. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie die Konferenz der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich haben sich mit dem Gesetzentwurf des BMI befasst, (vgl. Ziff. 22.7 und Ziff. 21.8 dieses Berichts). Ich habe die Senatorin für Finanzen und den Senator für Justiz und Verfassung darüber unterrichtet mit der Bitte, sich bei den Beratungen auf Bundesebene für eine Unterstützung der Forderungen einzusetzen.

19.3.5 Bericht über sonstige Themen aus der Arbeitsgruppe Auskunfteien

Von hervorgehobener Bedeutung in den Beratungen der AG Auskunfteien der Konferenz der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich waren insbesondere die datenschutzgerechtere Gestaltung der SCHUFA-Klausel und des SCHUFA-Merkblatts des Zentralen Kreditausschusses (ZKA), die Einhaltung datenschutzrechtlicher Anforderungen beim Abschluss von Verträgen mit Wohnungsunternehmen durch die SCHUFA und andere Auskunfteien sowie die Nutzung von Daten aus dem Inkassobereich für die Auskunftserteilung. Wie unter Ziff. 19.3.3 berichtet, bestand besonderer Erörterungsbedarf auch im Hinblick auf die beabsichtigte Änderung des Bundesdatenschutzgesetzes.

Außerdem wurden u. a. die Themen rechtliche Fragen der SCHUFA-Selbstauskunft, die Verwendung des Merkmals Versandhandelskonto im SCHUFA-Verfahren, das neue Konzept der SCHUFA bei nachträglichem Bestreiten von Forderungen, die Einwilligung bei der Übermittlung des SCHUFA-Scorewertes an B-Vertragspartner, die Speicherung von Voranschriften durch die SCHUFA, die Einbeziehung gespeicherter Merkmale in die SCHUFA-Scorewertberechnung sowie Datenschutz bei Detekteien näher beraten.

19.4 Bericht aus der Arbeitsgruppe Versicherungswirtschaft

Aus der Arbeit der AG Versicherungswirtschaft der Konferenz der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich sind zwei Themen herauszugreifen, die im Berichtsjahr intensiv behandelt wurden.

Seit geraumer Zeit verhandelt die AG Versicherungswirtschaft mit dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) über die Formulierung wirksamer Einwilligungs- und Schweigepflichtentbindungserklärungen für Versicherungsverträge. Die Verhandlungen über eine konsensfähige Schweigepflichtentbindungserklärung sind bereits weit fortgeschritten und können ggf. in Kürze zum Abschluss gebracht werden.

Weiterhin Schwerpunkt der Beratungen ist das Hinweis- und Informationssystem (HIS) des GDV. Dabei handelt es sich um eine Warndatei, in die Versicherungen Versicherte und Dritte (ggf. Unfallbeteiligte) nach einem Punktesystem einmelden, um Auffälligkeiten, die Hinweise auf Versicherungsbetrug begründen können, bei Haftungsfällen und Anträgen auf Vertragsabschluss abzurufen. Es zeichnen sich dabei Lösungen ab, die die Tätigkeit der Versicherungen klarer strukturiert und zugleich dabei entlastet. Der aktuelle Entwurf des GDV für eine Einwilligungserklärung kann zum jetzigen Zeitpunkt jedoch noch keine Zustimmung der AG Versicherungswirtschaft finden.

19.5 Ausstellung von Energieausweisen nach der Energieeinsparverordnung

Ende Juli 2007 ist die Energiesparverordnung (EnEV) in Kraft getreten. Unter den dort genannten Voraussetzungen sind Eigentümer von Wohnungen oder Häusern verpflichtet, einen Energiepass zu erstellen. Die Verordnung eröffnet dabei zwei Möglichkeiten: Die Erstellung eines bedarfsorientierten oder die Erstellung eines verbrauchsorientierten Energiepasses. Beim bedarfsorientierten Energiepass werden bestimmte objektive bauliche Gegebenheiten festgestellt. Anders ist es bei der Erstellung eines verbrauchsorientierten Energiepasses. Hier wird der konkrete Verbrauch der letzten drei Jahre der jeweiligen Wohneinheit zur Erstellung des Energiepasses herangezogen.

Vermieterorganisationen, Energieversorgungsunternehmen, Hausverwalter, Eigentümer wie auch Mieter wandten sich an mich und wollten wissen, inwieweit bei der Ausstellung eines verbrauchsabhängigen Energieausweises bei Etagenheizungen die Verbrauchsdaten der Mieter beim jeweiligen Energieversorger dort von dem Vermieter oder von dem Aussteller des Passes abgerufen bzw. vom Energieunternehmen übermittelt werden dürfen. Da weder die EnEV noch das zugrunde liegende Energieeinsparungsgesetz (EnEG) Datenverarbeitungsregelungen für die Erstellung eines Energiepasses enthalten, kommen die allgemeinen Regelungen des Bundesdatenschutzgesetzes (BDSG) zur Anwendung. Es ist sicherlich unstreitig, dass ein berechtigtes Interesse des Eigentümers bzw. des Vermieters an den Verbrauchsdaten besteht, es ist aber nicht ausgeschlossen, dass schutzwürdige Belange der Mieter dabei beeinträchtigt sein können. Auch darf nicht passieren, dass ohne Kenntnis der Mieter Daten zwischen Energieunternehmen und Dritten über das Verbrauchsverhalten der einzelnen Mietparteien ausgetauscht werden. Es gibt daher zwei Möglichkeiten, an die verbrauchsorientierten Daten zu gelangen:

Entweder der Mieter gibt seine Verbrauchsdaten unmittelbar an den Vermieter oder den von ihm beauftragten Gutachter oder aber er erklärt in einer schriftlichen Einwilligung, dass der Vermieter oder der Gutachter berechtigt sind, die für die Erstellung des Energiepasses erforderlichen Daten beim Energieunternehmen direkt abzufragen. Ist der Mieter nicht bereit, seine Daten für die Erstellung eines Energiepasses preiszugeben, verbleibt dem Vermieter oder Eigentümer nur die Möglichkeit, mit den ihm bekannten baulichen Daten einen bedarfsorientierten Energiepass ausstellen zu lassen.

19.6 Verarbeitung personenbezogener Daten bei der Bestellung von Fotos

Im Januar 2007 wandte sich ein Petent an mich und berichtete, dass bei dem geräteunterstützten Erstellen von Foto-CDs im Einzelhandel, um anschließend Abzüge anfertigen zu lassen, ohne dass der Kunde darauf hingewiesen wird, alle Daten von dem Speichermedium, z. B. einem USB-Stick, heruntergeladen und auf die Foto-CD gespeichert werden. Der Petent beklagte, dass dadurch nicht nur alle Fotos, unabhängig davon, ob nur Abzüge gewünscht werden, sondern auch alle weiteren, unter Umständen sehr sensiblen Daten des Speichermediums in die Hände der Mitarbeiter des Einzelhandelsgeschäfts und des von ihm beauftragten Entwicklungsbüros gelangen.

Ich habe mich im Februar 2007 hiervon bei einem in Bremen ansässigen Fotogeschäft überzeugt und mich anschließend an die Geschäftsführung des Unternehmens gewandt und datenschutzgerechte Verbesserungen vorgeschlagen. Das Unternehmen hat meine Auffassung aufgegriffen und war bereit, auf den Geräten die Kunden über das vollständige Auslesen hinzuweisen. Die Verpflichtung zu einer sofortigen technischen Umstellung aller Geräte hätte aber einen Wettbewerbsnachteil bedeutet, sofern nicht andere Unternehmen in anderen Bundesländern dieselbe Transparenz herstellen, denn die Geräte von einem Hersteller in Niedersachsen werden bundesweit 10.000- bis 20.000-fach im ganzen Einzelhandel eingesetzt.

Daraufhin habe ich die Aufsichtsbehörden für den Datenschutz der anderen Bundesländer informiert mit dem Ziel, eine bundesweit einheitliche Vorgehensweise abzustimmen. Zugleich habe ich den Landesbeauftragten für Datenschutz in Niedersachsen gebeten, bei dem Hersteller die Möglichkeit einer technischen Änderung anzusprechen, bei der nur die tatsächlich für die Bestellung ausgewählten Bilder auf die CD gespeichert werden.

Der Hersteller teilte mit, dass die Geräte durch eine neue Programmversion seit Mitte Februar 2007 grundsätzlich nur noch Foto- und Videodateien kopieren und zudem die Wahl zwischen Archiv-CD (alle Bilder und Videos) und Transfer-CD (nur die für die Abzugsbestellung erforderlichen Dateien) überlässt. Damit ist mittelfristig bundesweit eine datenschutzgerechte Umstellung der Geräte in Sicht.

19.7 Teilnahme an einem Gewinnspiel der Post

Viele Bewohner und Autofahrer in Bremen wurden von der Deutschen Post per Prospekt aufgefordert, an einem Gewinnspiel teilzunehmen. Es winkten 500 Kraftstoff-Gutscheine im Werte von je 50,-- €. Dabei wurde neben verschiedenen Fragen rund um das Auto und über den Haushalt auch nach der beruflichen Tätigkeit und dem Netto-Einkommen der Haushalte gefragt.

Ich habe auf Anfrage öffentlich davor gewarnt, der Post leichtfertig und ungeprüft eine Vielzahl von Daten aus dem persönlichen Lebensbereich preiszugeben, zumal die weitere Nutzung der Daten durch die Post nur sehr unbestimmt beschrieben war. Für die Teilnehmer war nicht einzuschätzen, an wen die Post die Daten übermitteln würde, mit welchen anderen Daten diese verknüpft und wie die Empfänger die Daten weiter verarbeiten oder nutzen würden. Auch bestanden Bedenken, ob die Einwilligungserklärung ausreichend war, die die Post berechtigte, die persönlichen Daten an unbekannte Stellen zu übermitteln. Zur Prüfung dieser Frage habe ich die zuständige Datenschutzaufsichtsbehörde, den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), eingeschaltet. Dieser hat gegenüber der Deutschen Post AG einige grundsätzliche Datenschutzverbesserungen durchgesetzt, die in Zukunft bei entsprechenden Aktionen beachtet werden sollen.

19.8 Arbeitnehmerdatenschutz

19.8.1 Prüfung der Beschäftigtendatenverarbeitung im Bewerbungsverfahren

In einem Betrieb mit mehreren 100 Beschäftigten prüfte ich schwerpunktmäßig die Datenerhebung im Bewerbungsverfahren. Hierbei ging es im Wesentlichen darum, ob und ggf. welche Gesundheitsdaten (Drogentest, ärztliche Untersuchung DNA-Analyse und Schwerbehinderung) erhoben werden, ob nach einer Schwangerschaft gefragt wird, ob psychologische Testverfahren oder ein graphologischer Test durchgeführt wird, ob Daten beim bisherigen Arbeitgeber und Angaben über die finanzielle Situation (Schulden, Lohn- und Gehaltspfändung), Angaben zur Gewerkschaftszugehörigkeit und über einen strafrechtlichen Hintergrund (polizeiliches Führungszeugnis, Vorstrafen, staatsanwaltschaftliches Ermittlungsverfahren) erhoben werden.

Im Rahmen eines Prüftermins wurde festgestellt, dass hinsichtlich der Gesundheitsdaten nur eine ärztliche Untersuchung nach dem Jugendarbeitsschutzgesetz durch den Betriebsarzt durchgeführt bzw. die Vorlage eines entsprechenden Nachweises verlangt wird. Weitere der vorgenannten Gesundheitsdaten und der übrigen Daten werden nicht erhoben. Auch eine Datenerhebung bei früheren Arbeitgebern wurde verneint.

Der zur Vorbereitung der Einstellung verwendete Personalfragebogen enthielt u. a. Felder zur Staatsangehörigkeit, zum Familienstand, Angaben zum Ehepartner (vollständiger Name, Geburtsname und -datum und Konfession), zu den Kindern den Vornamen und das Geburtsdatum) sowie im Zusammenhang mit einer Schwerbehinderung die Angaben „Kriegsschaden“ oder „Arbeitsunfall“, deren Berechtigung ich näher untersuchte.

Die Erforderlichkeit der Angaben und Rechtsgrundlagen zur Konfession und zum Familienstand sowie die Felder „Kriegsschaden“ oder „Arbeitsunfall“ konnten nicht dargelegt werden, so dass die entsprechenden Felder auf dem überarbeiteten Personalfragebogen nicht mehr vorhanden sind. Die Angaben zum Ehepartner und den Kindern werden für die Pensionskasse des Unternehmens benötigt. Das Unternehmen wird auf meine Anregung hin in dem überarbeiteten Personalfragebogen zu diesen Angaben darauf hinweisen, dass sie freiwillig sind und für welchen Zweck sie benötigt werden.

Insgesamt habe ich bei der Prüfung einen guten Eindruck gewonnen, es wurden nicht in großem Umfang Daten der Bewerber mit fraglicher Eignung erhoben, sondern im Mittelpunkt der Entscheidung stand der unmittelbare Eindruck, den die Bewerberinnen und Bewerber hinterließen.

19.8.2 Ortungssystem in Firmenfahrzeugen

Beschäftigte eines Bauunternehmens haben mich darüber unterrichtet, in den Fahrzeugen ihres Arbeitgebers seien Ortungssysteme eingebaut worden, mit denen er die Beschäftigten während der Arbeitszeit und der Pausen kontrollieren könne. Es bestünden Unsicherheiten darüber, was und ggf. in welchem Ausmaß der Arbeitgeber kontrollieren dürfe. Auf Anfrage hat der Arbeitgeber dargelegt, das eingesetzte GPS-System werde zur elektronischen Arbeitszeiterfassung, zur Disposition und zum Aufspüren von gestohlenen Fahrzeugen/Geräten eingesetzt und es handele sich dabei nicht um automatisierte Datenverarbeitung. In diesem Zusammenhang hat mir die Firma, von dem das Unternehmen das System erworben hat, Informationen (Broschüre, Muster einer Betriebsvereinbarung etc.) über das System zugesandt. Es ermöglicht in vielfältiger Weise eine Überwachung der Beschäftigten.

Ich habe dem Unternehmen mitgeteilt, dass dort ein Verfahren eingesetzt wird, mit dem Daten automatisiert verarbeitet werden, die regelmäßig auf einzelne Fahrer bzw. Beschäftigte des Unternehmens bezogen werden können. Da dieses Verfahren u. a. ein Bewegungsprofil der Fahrer ermöglicht, weist dieses DV-System besondere Risiken für die Rechte der betroffenen Fahrer auf. Deshalb unterliegt das Verfahren einer Prüfung, die vor Beginn der Verarbeitung (Vorabkontrolle) nach § 4 d Abs. 5 Satz 1 Bundesdatenschutzgesetz (BDSG), vom Beauftragten für den Datenschutz hätte vorgenommen werden müssen (§ 4 d Abs. 6 BDSG).

Dazu gehört insbesondere unter Abwägung mit den berechtigten Interessen des Arbeitgebers und den schutzwürdigen Interessen der betroffenen Fahrer entsprechend § 28 Abs. 1 Nr. 2 BDSG konkret festzulegen, welche Auswertungen vorgenommen werden. Dass es dabei bleibt, ist durch technische und organisatorische Maßnahmen nach § 9 BDSG zu gewährleisten, und die Beschäftigten sind nach § 33 BDSG über Inhalt und Umfang der Datenverarbeitung und der Datenspeicherung zu benachrichtigen. Ich habe das Unternehmen aufgefordert, dies entsprechend nachzuholen. Soweit ein Betriebsrat in solchen Unternehmen vorhanden ist, empfiehlt sich der Abschluss einer entsprechenden Betriebsvereinbarung.

19.8.3 Übermittlung von Beschäftigtendaten eines Sicherheitsdienstes

Der Betriebsrat eines Sicherheitsdienstes hat mich gefragt, ob und ggf. in welchem Umfang der Arbeitgeber Daten aus der Personalakte seiner Beschäftigten an einen Auftraggeber übermitteln darf und ob dies auch ohne die Zustimmung der Beschäftigten geschehen dürfe. Geplant war die Bereithaltung der Personalakte zur Einsichtnahme durch den Auftraggeber.

Es war zu prüfen, ob die Voraussetzungen des § 28 Abs. 3 Nr. 1 BDSG vorliegen. Danach dürfen personenbezogene Daten übermittelt werden, soweit sie zur Wahrung berechtigter Interessen eines Dritten (hier: Auftraggeber) erforderlich sind und kein Grund zu der Annahme besteht, dass der Betroffene (hier: Beschäftigte) ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Grundsätzlich besteht für den Auftraggeber das berechtigte Interesse, sich ein Bild von den Beschäftigten des Sicherheitsdienstes zu machen, die für den Schutz oder die Sicherung eines bestimmten Objektes eingesetzt werden sollen. Hierbei ist der Grundsatz der Erforderlichkeit zu beachten. Keine Bedenken bestehen, wenn die Namen der Beschäftigten und ggf. - bezogen auf das zu schützende oder sichernde Objekt – Daten über dessen Qualifikation übermittelt werden, soweit diese für den Einsatz vorausgesetzt werden. Angaben zur privaten Adresse oder Telefonnummer wären nur dann erforderlich, soweit die Beschäftigten regelmäßig, kurzfristig sowie außerhalb der regulären Geschäftszeiten erreichbar sein müssen. Die Funktion eines Beschäftigten darf allenfalls im Zusammenhang mit dem zu schützenden oder zu sichernden Objekt im erforderlichen Umfang mitgeteilt werden, z. B. bei Einsatz eines Teams dessen Leiter bzw. Vertreter.

Regelmäßig nicht erforderlich sind Angaben über Funktionen im Rahmen der Personalvertretung o. a., da diese nicht in einem unmittelbaren Zusammenhang mit dem zu schützenden oder zu sichernden Objekt stehen. Das Gleiche gilt für Angaben zum Geburtsdatum, zur Betriebszugehörigkeit und für evtl. regelmäßig einzuholende polizeiliche Führungszeugnisse oder Auskünfte von Auskunfteien, z. B. der SCHUFA. Hier dürfte es ausreichen, wenn der Sicherheitsdienst sich verpflichtet, nur Beschäftigte entsprechend einzusetzen, wenn die jeweiligen vertraglich festzulegenden Anforderungen erfüllt sind. Insoweit trägt der Sicherheitsdienst die Verantwortung, dass diese Verpflichtungen eingehalten werden. In diesem Sinne hat sich der anfragende Betriebsrat des Unternehmens eingesetzt.

19.9 Einsatz von Videoüberwachung

Im Berichtsjahr erreichte mich wiederum eine Vielzahl von Anfragen, die sich gegen eine Überwachung durch Videokameras wandten. Einige Beispiele sind nachstehend aufgeführt.

In einer Modeboutique: Aufgrund von Hinweisen Betroffener habe ich mir die Videoüberwachung in einem Modegeschäft in der Bremer Innenstadt vorführen lassen und bei der Einsichtnahme in die Bilddaten auf dem Monitor Folgendes festgestellt:

Ich prüfte die Überwachung der Beschäftigten. Neben dem Verkaufsraum wird auch der Bereich an der Kasse videoüberwacht. In diesem Bereich hält sich regelmäßig zumindest ein Mitarbeiter bzw. eine Mitarbeiterin auf, so dass diese Person einer ständigen Videoüberwachung und damit einem lückenlosen Überwachungsdruck ausgesetzt ist. Sie kann nämlich nicht einschätzen, ob und ggf. wann von wem und zu welchen Zwecken eine Einsichtnahme in die Bilddaten erfolgt. Insoweit überwiegen die schutzwürdigen Interessen des Beschäftigten, so dass die Voraussetzungen des § 6 b BDSG nicht erfüllt sind. Ich habe den Inhaber daher gebeten, die Videoüberwachung im Kassenbereich unverzüglich einzustellen und die damit bisher aufgenommenen Bilddaten zu löschen.

Ich prüfte die Hinweise auf die Videoüberwachung. Außer einem Hinweisschild mit einem Video-Logo an der Eingangstür des Verkaufsgeschäfts, das ich erst nach längerem Hinsehen und auf den Hinweis einer Mitarbeiterin erkennen konnte, gab es im Verkaufsbereich selbst keine weiteren Hinweise auf den Umstand der Videoüberwachung, obwohl § 6 b Abs. 2 BDSG vorschreibt, dass der Umstand und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen sind. Ich habe verlangt, durch deutliche Hinweisschilder auf die Videoüberwachung aufmerksam zu machen.

Ich prüfte die Dauer der Aufzeichnung der Bilddaten und Einsichtnahme. Unklar war, wie lange die Bilddaten aufgezeichnet werden. Zwar ist von der anwesenden Mitarbeiterin erklärt worden, die Aufnahmen würden elf Tage aufbewahrt werden, Unterlagen oder sonstige Dokumentationen standen jedenfalls nicht zur Verfügung. Da die Videoüberwachung im Wesentlichen der Abwehr von Diebstählen dienen soll, habe ich verlangt, die Aufzeichnungen entsprechend § 6 b Abs. 5 Bundesdatenschutzgesetz (BDSG) unverzüglich nach Erreichen des Zwecks durch eine automatische Einstellung zu löschen, regelmäßig spätestens nach drei Tagen.

Ich prüfte die Verfahrensbeschreibung. Auch war nicht festzustellen, ob und ggf. wer unter welchen Voraussetzungen Einsicht in die Bilddaten hat bzw. haben darf und ob diese Einsichtnahme auch außerhalb des Verkaufsgeschäftes, z. B. über eine externe Verbindung o. ä., möglich ist. Es wurde lediglich auf die Firma verwiesen, die die Anlage installiert hat. Eine Einweisung sei zwar beabsichtigt gewesen, bisher jedoch nicht erfolgt. Unterlagen darüber lagen ebenfalls nicht vor. Da es sich bei dieser Videoüberwachung um ein Verfahren automatisierter Verarbeitung handelt, ist der Inhaber nach § 4 d Abs. 1 BDSG verpflichtet, eine Verfahrensbeschreibung nach Maßgabe des § 4 e BDSG zu erstellen. Hierin ist auch festzulegen, ob und unter welchen Voraussetzungen eine Einsichtnahme durch wen erfolgt und welche technischen und organisatorischen Maßnahmen nach der Anlage zu § 9 Satz 1 BDSG getroffen werden, um dies zu gewährleisten.

In einer Fahrradstation: Ich bin darüber unterrichtet worden, auf die Videoüberwachung einer Fahrradstation am Bremer Hauptbahnhof würde nicht hingewiesen. Aufgrund meiner Anfrage wurde

mir erklärt, es seien nunmehr Hinweise angebracht. Die nur außerhalb der Geschäftszeiten aktivierte Aufzeichnung von Bilddaten würde bis zu zwei Monate aufbewahrt werden.

Ich habe auf § 6 b Abs. 5 Bundesdatenschutzgesetz (BDSG) hingewiesen, wonach Aufzeichnungen unverzüglich zu löschen sind, wenn sie zur Erreichung des Zieles nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Nach allgemeiner Erfahrung werden Einbrüche und Diebstähle regelmäßig am nächsten Arbeitstag zu Beginn der Geschäftszeiten festgestellt. In diesen Fällen dürfen die Aufnahmen zur Verfolgung straf- und zivilrechtlicher Ansprüche eingesehen und ausgewertet werden. Hierbei besteht regelmäßig die technische Möglichkeit, die entsprechende Sequenz auszuschneiden und separat für die genannten Zwecke zu verwenden. Die übrigen Aufnahmen sind dann unverzüglich zu löschen.

Ich habe daher gebeten, für die Aufzeichnung eine Löschungsfrist von 24 Stunden technisch und organisatorisch zu gewährleisten. Nur in dem Fall, dass die Radstation am Wochenende oder an Feiertagen geschlossen ist, wäre eine Löschungsfrist von bis zu drei Tagen angemessen. Weiter habe ich eine Verfahrensbeschreibung nach § 4 e i. V. m. § 6 b BDSG gefordert. Dies wurde zugesichert.

19.10 Ordnungswidrigkeitsverfahren

Bei der Durchführung von Ordnungswidrigkeitsverfahren wird nur gelegentlich eine richterliche Entscheidung erforderlich. Es ist daher kein Wunder, dass in solchen Fällen die mit dem Verfahren betrauten Richterinnen und Richter, aber auch Staatsanwältinnen und Staatsanwälte mit der datenschutzrechtlichen Materie nur wenig vertraut sind. Häufig sind die Genannten auf Massenverfahren wie Verkehrsordnungswidrigkeiten spezialisiert, so dass das Verständnis für datenschutzrechtliche, insbesondere aber für datenschutztechnische Fallkonstellationen nur eingeschränkt vorhanden ist.

Um die Gerichte und Staatsanwaltschaften bei der Bearbeitung von Ordnungswidrigkeiten nach dem Bundesdatenschutzgesetz besser unterstützen zu können, haben sich die obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich im Berichtsjahr nun darauf verständigt, eine gemeinsame Urteilssammlung aufzubauen, in die von ihnen alle erfolgreich abgeschlossenen Ordnungswidrigkeitsverfahren eingemeldet werden. Die vom Hamburgischen Datenschutzbeauftragten geführte Sammlung ist außerdem geeignet, eine vergleichbare Behandlung von Ordnungswidrigkeitstatbeständen über die Ländergrenzen hinweg zu ermöglichen und Ordnungswidrigkeitsverfahren gezielter einzusetzen.

Im Berichtsjahr erließ ich nur einen Bußgeldbescheid wegen der Nichterteilung von Auskünften gegen den Geschäftsführer eines Unternehmens. Trotz mehrfacher Aufforderung und Fristsetzung, mir die erforderlichen Auskünfte zu der von ihm betriebenen Videoüberwachung zukommen zu lassen, bekam ich diese von dem betreffenden Unternehmen nicht. Letztendlich hat der Beschuldigte das gegen ihn verhängte Bußgeld bezahlt.

20. Schlussbemerkungen

20.1 Pflege und Entwicklung der Datenschutz-Homepage

Die Seiten meiner Homepage datenschutz.bremen.de, informationsfreiheit.bremen.de und datenschutz4school.de werden im Monat von ca. 19.000 Usern besucht, wobei die Datenschutzseite zu meiner am besten besuchten Seite gehört. Die am häufigsten ausgewählten Menüpunkte sind „Tipps für Bürger, Gesetzestexte und Veröffentlichungen“. Über 65 % der Besucher kommen über die Suchmaschine Google auf meine Seiten, viele auch über das Virtuelle Datenschutzbüro und einige über das Bremen.de-Portal. Die Seite www.datenschutz4school.de, die eine Lerneinheit enthält, wurde in den letzten beiden Monaten 820-mal aufgerufen. Um auch auf meinen anderen Homepageseiten einen besseren Überblick über Besucherzahlen zu bekommen, startet zum 1. Januar 2008 ein Besucherzähler.

Meine Homepageseiten wurden in diesem Jahr umfangreich überarbeitet. Auf der Datenschutzseite wurden allein drei neue Orientierungshilfen aufgenommen, und zwar die Orientierungshilfe „Datenschutzgerechter Einsatz von RFID“ sowie eine „Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ und eine Anleitung zur Entwicklung eines Konzeptes zur Löschung und Datenträgervernichtung durch Behörden und Unternehmen.

Unter „Tipps für Bürger“ wurden fünf neue Artikel zum Thema Arbeitnehmerdatenschutz veröffentlicht, sie geben Hinweise und Verhaltensregeln für beschäftigte, aber auch für Arbeitgeber unter den folgenden Titeln: „Firmeninterne Warnsysteme und Beschäftigtendatenschutz“, „Erhebung von Gesundheitsdaten im Bewerbungsverfahren“, „Videoüberwachung am Arbeitsplatz“, „Namensschilder auf Arbeitskleidung“ und „E-Mail-Weiterleitung nach Ausscheiden eines Mitarbeiters aus dem Betrieb?“. Die Bereiche „Selbstverteidigung im Internet“ und „Gesetze“ wurden fast komplett überarbeitet und ausgebaut. Außerdem wurden Teile der CD „25 Jahre Datenschutz in Bremen“ auf meiner Homepage abgebildet. Damit wurden Empfehlungen Rechnung getragen, auch die historische Entwicklung des Datenschutzes in Bremen zu dokumentieren.

20.2 Schriftliche Eingaben und Anfragen

Die Zahl der schriftlichen Eingaben per Brief, immer häufiger aber auch per E-Mail oder Fax, und die telefonischen Anfragen von Bürgerinnen und Bürgern, die die Datenverarbeitung von Behörden, Unternehmen oder anderen Stellen betreffen, stieg im Jahr 2007 weiter an. Besonders häufig betrafen die Eingaben im öffentlichen Bereich Fragen der Personaldatenverarbeitung. Darüber hinaus hatten, wie bereits im Vorjahr, die Datenverarbeitung der Polizei und der Bereich Jugend, Familie und Soziales, speziell die BAgIS, einen hohen Anteil. Eine erhebliche Anzahl der Eingaben richtete sich auf die Verarbeitung personenbezogener Daten in den Schulen und in der Schulverwaltung.

Im nicht öffentlichen Bereich hatten Fragen besonderen Anteil an den Eingaben, die den Arbeitnehmerdatenschutz, die Datenverarbeitung im Bereich der Kreditwirtschaft/Auskunfteien, die Verarbeitung von Mieterdaten sowie die Videoüberwachung betrafen.

Eine Auswahl der telefonischen Anfragen, die ich im Berichtsjahr erhielt und die bereits im Telefongespräch mit dem Anrufer beantwortet werden konnten, habe ich wieder in einer Tabelle diesem Bericht als Anlage beigefügt (vgl. Ziff. 24.2).

20.3 Öffentlichkeitsarbeit, Vorträge, Fortbildungsangebote und Kooperationen

Die meisten Bürgerinnen und Bürger erreiche ich sicherlich mit meinem Internetauftritt www. datenschutz.bremen.de. Das verdeutlicht die Zahl von 19.000 Zugriffen auf meine verschiedenen Internet-Seiten, wobei der Datenschutz den Hauptanteil hat. Bei telefonischen Anfragen oder Eingaben per Mail erfahre ich häufig positive Anerkennung für die Inhalte, auch wenn das Design der Seiten schon etwas in die Jahre gekommen ist. Es gilt diesen Bereich noch weiter auszubauen, um eine noch bessere Beratung der Bürger zu erzielen und gleichzeitig meine Dienststelle von weiteren allgemeinen Anfragen zu entlasten. Leider musste ich die Aktualisierung und Fortentwicklung meiner Internet-Seiten für den Datenschutz zugunsten des Aufbaus der Internetseite für die Informationsfreiheit im letzten Jahr zurückstellen und auch im Berichtsjahr waren hierfür nicht genügend Kapazitäten frei. Ein Stück weit hilft hier die vom „Virtuellen Datenschutzbüro“ betriebene "Frontpage" der Datenschutzbeauftragten und der Kooperationspartner www.datenschutz.de mit brandaktuellen Themen weiter, die ich ebenfalls unterstütze.

Die Zusammenarbeit mit den Datenschutzbeauftragten des Bundes und der Länder, mit den obersten Datenschutzaufsichtsbehörden in verschiedenen Gremien, mit Verbänden und anderen Organisationen erleichtert häufig die Aufgabe, Datenschutzforderungen zu präzisieren, aber auch im Bundesgebiet zu vereinheitlichen wie auch die Anforderungen des Datenschutzes „in die Fläche zu bringen“. Gastreden wie z. B. zum 30-jährigen Bestehen des Erfa-Kreises Bremen/Weser-Ems, dem organisatorischen Zusammenschluss der hier tätigen betrieblichen Beauftragten für den Datenschutz, sind neben der regelmäßigen Teilnahme an deren Sitzungen ebenso unter diesem Punkt zu erwähnen wie die Mitwirkung im Rahmen einer Veranstaltung „Jugend im Parlament“ oder die durchgeführten Fortbildungsveranstaltungen der BAgIS-Teamleiter oder der behördlichen Beauftragten für den Datenschutz in Bremerhaven und Bremen .

Schließlich ist die Pressearbeit ein wichtiges Instrument, um auf aktuelle Themen zu reagieren, die von mir herausgegebenen Pressemitteilungen sind auf meiner Internetseite veröffentlicht. Da die Diskussion um Fragen des Datenschutzes und der inneren Sicherheit in 2007 teilweise sehr stark eskalierte, wurde ich auch mehrfach um Interviews von der lokalen Presse, aber auch von Hörfunk und Fernsehen gebeten. Immer wieder beeindruckend finde ich dabei, dass nach Erscheinen der Presse oder Ausstrahlung der Sendung sich oft eine ganze Reihe von Bürgern bei mir melden und über ihre oft aktuellen negativen Erfahrungen, verursacht durch elektronische Datenverarbeitung, berichten und um Rat fragen. Eine Übersicht über die im Berichtsjahr erschienenen Berichte mit Datenschutzthemen oder mit Datenschutzbezug in Presseorganen der Region befindet sich im Anhang (vgl. Ziff.24.1 dieses Berichts).

20.4 Zur Situation der Dienststelle

In einem Horoskop für 2007 wurde für mein Sternzeichen Folgendes prophezeit: „Ihre Kollegen verweigern die Mitarbeit, weil Sie ihnen zuviel Arbeit aufgebürdet haben. Sie werden wohl oder übel einen Teil der Aufgaben selbst erledigen müssen." Und so ähnlich kam es denn auch. Es war zwar nur ein Wochenhoroskop, es sollte aber für das ganze Jahr seine Gültigkeit behalten. Nicht, dass von den mir verbleibenden Kolleginnen und Kollegen die Mithilfe verweigert wurde, sondern trotz Überstunden und Beschränkung auf das Allernötigste war die Arbeit nicht mehr zu schaffen. Belastet durch drei Beschäftigte in der Freistellungsphase der Altersteilzeit und bedingt durch eine Elternzeit nach Entbindung standen zum Anfang des Berichtsjahres für sechs juristische Referate noch gerade einmal zwei Referenten zur Verfügung. Dieses Verhältnis verbesserte sich dann im Laufe des Jahres auf drei für sechs und ab September 2007 auf vier für sechs, wobei jeweils eine Referentin bzw. ein Referent nicht mit voller Stundenzahl zur Verfügung stehen. Hinzu treten die insoweit noch zusätzlichen Belastungen aus dem in 2006 neu hinzugekommenen Bereich der Informationsfreiheit (vgl. meinen dazu separat abgegebenen 2. Jahresbericht). Wenn also im Bericht über Aktivitäten in einigen Ressorts so gut wie nichts berichtet wird und im Bereich der Privatwirtschaft Prüfungen nur in ganz geringem Umfang durchgeführt werden konnten, so liegt dies an dem Umstand, dass in einer so kleinen Dienststelle wie meiner durch Umsteuerungen Ausfälle nicht mehr aufgefangen werden können.

In den letzten Jahren wurde in der Dienststelle eine ganze Reihe von Sparmaßnahmen durchgeführt. Die Möglichkeiten wurden hierbei ausgeschöpft. Die besonderen Probleme, die sich durch das Fehlen von Arbeitskräften, die sich in der Freistellungsphase der Altersteilzeit befinden, ergeben, werden anhalten. Eine vorübergehende personelle Kompensation ist weiterhin unbedingt erforderlich. Zu bemerken ist, dass immer mehr Gesetze sehr differenzierte Datenschutzregelungen enthalten, die u. a. mit der Vorgabe von Parlament und Regierung in Kraft gesetzt werden, die Einhaltung wird von den Datenschutzbeauftragten kontrolliert. Die drastische Zunahme der Zahlen bei der Kontenabfrage und der Telefonüberwachung oder der vielfältigen Datenaustauschregelungen zwischen Polizei und Nachrichtendiensten, um nur einige zu nennen, erfordern Datenschutzkontrollen im Lande, die ich mit Vertretungsregelungen nicht durchführen kann. Fakt ist auch, dass die Bremer Wirtschaft auf ihre Datenschutzfragen von mir zeitnahe Entscheidungen erwartet. Der wirtschaftliche Erfolg hängt oft mit gutem Datenschutz, aber auch vom Zeitpunkt der Einführung einer Dienstleistung oder eines Produktes auf dem Markt ab. Es gibt zahlreiche weitere Entwicklungen, insbesondere im Bereich der IuK-Technologien, die sogar einen erhöhten Personaleinsatz erfordern.

Von den Fischen kann man nicht erwarten, dass sie für den Fischer mehr Netze verlangen. In den senatorischen Ressorts soll ich Kontrollen ausüben. Dass der Senat meine Dienststelle stärkt, kann ich nicht erwarten. Natürlicher Verbündeter war früher das Parlament, bedauerlicher Weise hat der Haushaltsausschuss in Kenntnis der eingangs geschilderten katastrophalen personellen Situation meiner Dienststelle für 2006/2007 keine Unterstützung gewährt. Leider sehen die vom Senat für den kommenden Doppelhaushalt vorgelegten Zahlen des PEP für meine Dienststelle vor, die Beschäftigtenzielzahl mit höchster Quote weiter zu senken.

21. Die Entschließungen der Datenschutzkonferenzen im Jahr 2007

21.1 Anonyme Nutzung des Fernsehens erhalten!

(Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2007)

Seit einiger Zeit werden in der Öffentlichkeit Pläne der großen privaten Fernsehveranstalter diskutiert, gemeinsam mit den Betreibern von Übertragungskapazitäten (Satellit, Kabel und DVB-T) ihre Programme nur noch verschlüsselt zu übertragen. Dabei werden vorrangig solche Geschäftsmodelle favorisiert, bei denen die kostenpflichtige Entschlüsselung des Signals nur mit personenbezogenen Smartcards möglich sein soll.

Die Datenschutzbeauftragten des Bundes und der Länder betrachten diese Entwicklung mit Sorge. Nachdem vor allem durch zahlreiche staatliche Eingriffe die verfassungsrechtlich gebotene unbeobachtete Nutzung von Telekommunikation und Internet kaum noch möglich ist, steht nun auch der seit jeher selbstverständliche anonyme und nicht registrierte Empfang von Rundfunkprogrammen auf dem Spiel. Gerade durch die Vermarktung individuell zugeschnittener Programmpakete im digitalen Rundfunk kann bei personenbezogener Abrechnung nachvollzogen werden, wer welche Angebote nutzt. Die entstehenden technischen Infrastrukturen werden zudem auch Möglichkeiten bieten, die konkrete Nutzung einzelner Sendungen zu registrieren. Damit wird die allgegenwärtige Bildung von Persönlichkeitsprofilen um detaillierte Kenntnisse über den Rundfunkkonsum ergänzt.

Die bisher bekannt gewordenen Pläne der Unternehmen widersprechen dem im Rundfunkstaatsvertrag geregelten Gebot, die Inanspruchnahme von Rundfunk und deren Abrechnung anonym zu ermöglichen, und verstoßen gegen das Prinzip der Datenvermeidung. Dies wäre nicht akzeptabel, zumal datenschutzfreundliche Varianten der Abrechnung – beispielsweise durch den Einsatz von vorbezahlten Karten – ohne wirtschaftliche Einbußen zur Verfügung stehen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb die Länder auf, die Einhaltung der datenschutzrechtlichen Anforderungen des Rundfunkstaatsvertrages gegenüber den Veranstaltern durchzusetzen und eine anonyme Nutzung von Rundfunkprogrammen auch in Zukunft sicherzustellen.

Angesichts der immer umfassenderen Individualisierung und Registrierbarkeit des Mediennutzungsverhaltens erinnert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an ihre Forderung, das grundgesetzlich geschützte Fernmeldegeheimnis zu einem allgemeinen Mediennutzungsgeheimnis weiterzuentwickeln.

21.2 Keine heimliche Online-Durchsuchung privater Computer

(Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2007)

Bisher ist nur die offene Durchsuchung privater Computer gesetzlich geregelt. Trotzdem wollen staatliche Behörden auch heimliche Online-Durchsuchungen durchführen. Bei einer Online-Durchsuchung dringen Sicherheitsbehörden mittels sog. „Trojaner“ heimlich in den Rechner ein und verschaffen sich Zugriff auf alle gespeicherten Daten.

Der Bundesgerichtshof hat in seinem Beschluss vom 31. Januar 2007 (StB 18/06) die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt, dass eine heimliche Online-Durchsuchung im Bereich der Strafverfolgung rechtswidrig ist. Weder die Bestimmungen zur Wohnungsdurchsuchung noch zur Telekommunikationsüberwachung können zur Rechtfertigung der heimlichen Durchsuchung und Ausforschung privater Computer herangezogen werden.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Einführung entsprechender Eingriffsgrundlagen sowohl im repressiven als auch im präventiven Bereich. Sie appellieren an die Gesetzgeber, es beim bisherigen Rechtszustand des „offenen Visiers“ zu belassen. Der Staat darf nicht jede neue technische Möglichkeit ungeachtet ihrer Eingriffstiefe zur Ausforschung einsetzen. Dies gilt auch dann, wenn wichtige Belange, wie z. B. die Strafverfolgung, betroffen sind. Hier ist ein Umdenken erforderlich. Es muss ein Raum der Privatsphäre bleiben, der nicht durch heimliche staatliche Überwachungsmaßnahmen ausgehöhlt werden darf.

Eine heimliche Online-Durchsuchung greift tief in die Privatsphäre ein. Die auf einem Computer gespeicherten Daten können aufgrund ihrer Vielzahl und besonderen Sensibilität Einblick in die Persönlichkeit der Betroffenen geben. Der Schutz des Kernbereichs privater Lebensgestaltung wird gefährdet, wenn der Staat heimlich und fortdauernd in private Computer eindringt, um dort personenbezogene Daten auszuspähen. Dies gilt umso mehr, wenn Nachrichtendienste die Möglichkeit heimlichen Zugriffs auf diese Informationen erhalten, obwohl ihnen nicht einmal die offene Erlangung durch eine Beschlagnahme gestattet ist.

Es ist Aufgabe des Staates dafür Sorge zu tragen, dass den Einzelnen die Möglichkeit zur Entfaltung ihrer Persönlichkeit bleibt. Diese Möglichkeit würde unvertretbar eingeschränkt, wenn Durchsuchungsmaßnahmen zugelassen würden, bei denen aufgrund ihrer Heimlichkeit keine Person wissen kann, ob, wann und in welchem Umfang sie von ihnen bereits betroffen ist oder in Zukunft betroffen sein wird. Der Gesetzgeber sollte deshalb davon absehen, derartige neue Eingriffsbefugnisse zu schaffen, nur weil sie ihm technisch möglich erscheinen und ihre Zweckmäßigkeit behauptet wird. Die technische Entwicklung allein kann nicht der Maßstab für die Rechtfertigung von Eingriffen sein.

Die Konferenz befürchtet massive Sicherheitseinbußen, weil zu erwarten ist, dass sich Computernutzer vor staatlicher Ausforschung zu schützen versuchen, indem sie etwa Softwaredownloads unterlassen. Somit werden aber auch die sicherheitstechnisch wichtigen Software-Updates verhindert und Computer anfälliger gegen Angriffe Krimineller. Die Einführung von Befugnissen zur Online-Durchsuchung würde das Ansehen des Rechtsstaats und das Vertrauen in die Sicherheit von Informationstechnik, insbesondere von E-Government und E-Commerce, massiv

beschädigen. Schließlich würden die hohen Aufwendungen für IT-Sicherheit in Staat und Wirtschaft konterkariert. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert deshalb an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung derartiger Befugnisnormen zu verzichten.

21.3 Pläne für eine öffentlich zugängliche Sexualstraftäterdatei verfassungswidrig

(Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2007)

In der aktuellen Diskussion um einen verbesserten Schutz von Kindern vor Sexualstraftätern wird u. a. die Einrichtung einer öffentlich zugänglichen Sexualstraftäterdatei mit Wohnsitzangaben gefordert. Es wird vorgeschlagen, die Namen und Adressen von verurteilten Sexualstraftätern z. B. über das Internet zu veröffentlichen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont, dass an Kindern begangene Sexualstraftaten mit allen zur Verfügung stehenden rechtsstaatlichen Mitteln bekämpft werden müssen. Dies schließt jedoch die Anwendung eindeutig rechtsstaatswidriger Mittel aus. Um ein solches verfassungswidriges Mittel würde es sich aber bei einer solchen Datei handeln. Dadurch würden die Betroffenen an eine Art elektronischen Pranger gestellt. Sie würden durch die öffentliche Bloßstellung sozial geächtet. Tätern würde die Möglichkeit der Resozialisierung genommen, die ihnen nach unserer Rechtsordnung zusteht.

Der Vorschlag ist lediglich dazu geeignet, Misstrauen und Selbstjustiz zu fördern. Die Betroffenen könnten damit eher zu einem erhöhten Gefahrenpotenzial werden. Er sollte deshalb nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder nicht weiter verfolgt werden.

21.4 Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen

(Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2007)

Die gesetzlichen Regelungen der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sollen nach der Ankündigung der Bundesregierung unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts einer umfassenden Neuregelung unterzogen werden. Die Bundesregierung will in diesem Zusammenhang auch die europäische Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten umsetzen. Das Bundesministerium der Justiz hat zwischenzeitlich einen Referentenentwurf vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont erneut, dass die Vorratsdatenspeicherung deutschem Verfassungsrecht widersprechen würde. Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt. Die Konferenz fordert die Bundesregierung auf, die Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung zumindest so lange zurückzustellen, bis der bereits angerufene Europäische Gerichtshof über deren Rechtmäßigkeit entschieden hat.

Die geplante Ausweitung der Vorratsdatenspeicherung geht weit über die europarechtliche Umsetzungsverpflichtung hinaus und wäre ein zusätzlicher unverhältnismäßiger Eingriff in die Kommunikationsfreiheit der Bürgerinnen und Bürger. So sollen die Daten auch zur Verfolgung von Straftaten von erheblicher Bedeutung sowie mittels Telekommunikation begangener Straftaten genutzt werden. Zudem soll die Möglichkeit zur anonymen E-Mail-Kommunikation abgeschafft und die Nutzenden öffentlich zugänglicher E-Mail-Dienste sollen zur Angabe ihres Namens und ihrer Adresse verpflichtet werden. Diese Angaben sollen außerdem einer Vielzahl von Behörden zum Online-Abruf zur Verfügung gestellt werden, darunter der Polizei, den Staatsanwaltschaften, den Nachrichtendiensten, dem Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht. Auch dies begegnet erheblichen datenschutzrechtlichen Bedenken.

Zwar stärken einige der vorgesehenen Änderungen der Strafprozessordnung die rechtsstaatlichen und grundrechtlichen Sicherungen bei verdeckten strafprozessualen Ermittlungsmaßnahmen . Es besteht jedoch noch erheblicher Verbesserungsbedarf, insbesondere im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung, den Schutz von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern und die Voraussetzungen der Telekommunikationsüberwachung:

- Mit einer erneuten Ausweitung des Straftatenkatalogs für die Telekommunikationsüberwachung würde die Tendenz zunehmender Überwachungsmaßnahmen in verstärktem Maße fortgesetzt. Der Katalog sollte deshalb mit dem Ziel einer deutlichen Reduzierung kritisch überprüft werden. Es sollten nur Straftaten aufgenommen werden, deren Aufklärung in besonderem Maße auf die Telekommunikationsüberwachung angewiesen ist, die mit einer bestimmten gesetzlichen Mindeststrafe (z. B. ein Jahr) bedroht sind und die auch im Einzelfall schwer wiegen.

- Die vorgesehene Kernbereichsregelung ist ungenügend. Sie nimmt in Kauf, dass regelmäßig auch kernbereichsrelevante Informationen erfasst werden. Für solche Informationen muss stattdessen grundsätzlich ein Erhebungsverbot gelten. Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung, die dennoch erlangt werden, müssen zudem einem absoluten Verwertungsverbot unterliegen, nicht nur für Strafverfahren.

- Der Schutz des Kernbereichs privater Lebensgestaltung ist nicht nur in den Bereichen der Wohnraum- und Telekommunikationsüberwachung zu gewährleisten. Auch für alle anderen verdeckten Ermittlungsmaßnahmen ist eine Regelung zum Schutz des Kernbereichs zu treffen.

- Für die Kommunikation mit Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern sollte ein absolutes Erhebungs- und Verwertungsverbot geschaffen werden, das dem jeweiligen Zeugnisverweigerungsrecht entspricht. Dieses sollte unterschiedslos für alle Berufsgeheimnisträgerinnen und Berufsgeheimnisträger und deren Berufshelferinnen und Berufshelfer gelten. Die im Entwurf enthaltene Differenzierung zwischen bestimmten Gruppen von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern ist sachlich nicht gerechtfertigt.

- Für Angehörige i. S. v. § 52 StPO sollte ein Erhebungs- und Verwertungsverbot für die Fälle vorgesehen werden, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt. Die besonderen verwandtschaftlichen Vertrauensverhältnisse dürfen nicht ungeschützt bleiben.

- Für teilnehmende Personen von Kernbereichsgesprächen, die weder Berufsgeheimnisträgerinnen und Berufsgeheimnisträger noch Angehörige i. S. v. § 52 StPO sind, sollte insoweit ein Aussageverweigerungsrecht aufgenommen werden. Andernfalls bleibt der Kernbereich teilweise ungeschützt.

- Für die sog. Funkzellenabfrage, die alle Telefonverbindungen im Bereich einer oder mehrerer Funkzellen erfasst, sollten klare und detaillierte Regelungen mit engeren Voraussetzungen normiert werden. Diese sollten vorsehen, dass im Rahmen einer besonderen Verhältnismäßigkeitsprüfung die Anzahl der durch die Maßnahmen betroffenen unbeteiligten Dritten berücksichtigt und die Maßnahme auf den räumlich und zeitlich unbedingt erforderlichen Umfang begrenzt wird. Die Unzulässigkeit der Maßnahme zur Ermittlung von Tatzeuginnen und Tatzeugen sollte ins Gesetz aufgenommen werden.

- Die aufgrund einer Anordnung der Staatsanwaltschaft bei Gefahr in Verzug erlangten Daten dürfen nicht verwertet werden, wenn die Anordnung nicht richterlich bestätigt wird. Dieses Verwertungsverbot darf nicht - wie im Entwurf vorgesehen - auf Beweiszwecke begrenzt werden.

- Art und Umfang der Begründungspflicht für den richterlichen Beschluss der Anordnung der Telekommunikationsüberwachung sollte wie bei der Wohnraumüberwachung im Gesetz festgeschrieben werden. Im Sinne einer harmonischen Gesamtregelung sollten darüber hinaus qualifizierte Begründungspflichten für sämtliche verdeckte Ermittlungsmaßnahmen geschaffen werden.

- Zur Gewährleistung eines effektiven Rechtsschutzes ist sicherzustellen, dass sämtliche Personen, die von heimlichen Ermittlungsmaßnahmen betroffen sind, nachträglich von der Maßnahme benachrichtigt werden, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Darüber hinaus sollte bei Massendatenerhebungen

über eine ergänzende Benachrichtigung durch eine öffentliche Bekanntmachung der Maßnahme nachgedacht werden.

- Die für die Telekommunikationsüberwachung vorgesehenen Berichts- und Statistikpflichten sollten um Angaben zur Dauer der Überwachung, zur Anzahl der Gespräche und zur Benachrichtigung Betroffener ergänzt werden.
- Die im Entwurf enthaltenen erweiterten Eingriffsgrundlagen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden.

21.5 GUTE ARBEIT in Europa nur mit gutem Datenschutz

(Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2007)

Die Ministerinnen und Minister für Beschäftigung und Soziales in Europa haben am 19. Januar 2007 neun Schlussfolgerungen für GUTE ARBEIT aufgestellt: GUTE ARBEIT bedeute Arbeitnehmerrechte und Teilhabe, faire Löhne, Sicherheit und Gesundheitsschutz bei der Arbeit sowie eine familienfreundliche Arbeitsorganisation. Gute und faire Arbeitsbedingungen sowie angemessener sozialer Schutz seien unabdingbar für die Akzeptanz der Europäischen Union bei den Bürgerinnen und Bürgern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt diese Initiative zum Anlass und fordert dazu auf, auch den Beschäftigtendatenschutz zu stärken. Angesichts stetig wachsender technischer Möglichkeiten muss klar geregelt werden, welche Daten Unternehmen über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen.

Deshalb fordert die Konferenz seit langem ein Arbeitnehmerdatenschutzgesetz. Bereits 2003 hat sie darauf hingewiesen, dass Persönlichkeitsrechte und Datenschutz im Arbeitsverhältnis vielfältig bedroht sind, zum Beispiel durch

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

Die Achtung des Grundrechts auf informationelle Selbstbestimmung der Arbeitnehmerinnen und Arbeitnehmer zählt ebenso zu guten und fairen Arbeitsbedingungen wie Chancengleichheit oder gerechte Bezahlung. Beschäftigtendatenschutz erhöht zudem die Motivation, trägt und fördert die Arbeitszufriedenheit und bedeutet damit einen nicht zu unterschätzenden Standortvorteil.

Die Konferenz fordert die Bundesregierung auf, sich für einen hohen gemeinsamen Mindeststandard des Arbeitnehmerdatenschutzes in Europa einzusetzen und in Deutschland zeitnah einen entsprechenden Gesetzentwurf vorzulegen.

21.6 Elektronischer Einkommensnachweis muss in der Verfügungsmacht der Betroffenen bleiben

(Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2007)

Mit dem Verfahren ELENA (elektronische Einkommensnachweise) sollen die Einkommensdaten sämtlicher abhängig Beschäftigter in einem bundesweiten Register gespeichert werden. Dieses Verfahren ist angesichts der Sensibilität und des Umfangs der dabei erfassten personenbezogenen Daten von erheblicher datenschutzrechtlicher Brisanz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass ein derartiges Register nur dann eingerichtet werden darf, wenn die verfassungsrechtlichen Voraussetzungen erfüllt und die gesetzlichen und technisch-organisatorischen Vorkehrungen zum Schutz der dort gespeicherten Daten getroffen werden.

Zu den wesentlichen verfassungsrechtlichen Voraussetzungen für die Einrichtung des Registers gehören der Nachweis der Erforderlichkeit und die Verhältnismäßigkeit. Angesichts bestehender Zweifel daran, dass diese Voraussetzungen gegeben sind, muss belastbar dargelegt werden, dass die Daten für die jeweiligen Zwecke tatsächlich benötigt werden und dass der angestrebte Zweck nicht mit einem geringeren Eingriff in das Recht auf informationelle Selbstbestimmung erreicht werden kann.

Im Hinblick auf den vom Bundesministerium für Wirtschaft und Technologie erarbeiteten Referentenentwurf sieht die Konferenz darüber hinaus in den folgenden Punkten Klärungsbedarf:

- Es muss gesetzlich festgelegt werden, dass die Daten aus der Datenbank nur mit Mitwirkung der Teilnehmerinnen und Teilnehmer des Verfahrens zu entschlüsseln sind.
- Das Verfahren muss so ausgestaltet werden, dass die Ver- und Entschlüsselung der Daten ohne Vorliegen der Signaturkarte des Betroffenen nur in klar definierten Ausnahmefällen durch eine unabhängige Treuhänderstelle möglich ist.
- Sämtliche im Rahmen des Verfahrens verarbeiteten Daten müssen einem gesetzlichen Beschlagnahmeschutz unterworfen sein.
- Die technischen Komponenten müssen auf der Basis einer unabhängigen Prüfung zertifiziert werden.

21.7 Telekommunikationsüberwachung und heimliche Ermittlungsmaßnahmen dürfen Grundrechte nicht aushebeln

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. Juni 2007 im Umlaufverfahren)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wendet sich mit Nachdruck gegen die von Bundesregierung und Bundesratsgremien geplante Einführung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und die Verschärfungen verdeckter Ermittlungsmaßnahmen, vor allem durch Telekommunikationsüberwachung:

Die Datenschutzbeauftragten haben am 8./9. März 2007 auf ihrer Konferenz in Erfurt einen ersten Gesetzentwurf als verfassungswidrig beanstandet. Insbesondere haben sie vor heimlichen Online-Durchsuchungen und der Vorratsdatenspeicherung gewarnt. Damit würde tief in die Privatsphäre eingegriffen und das Kommunikationsverhalten der gesamten Bevölkerung – ob via Telefon oder Internet – pauschal und anlasslos erfasst.

Die einhellige Kritik der Datenschutzbeauftragten und ihre Aufforderung, stattdessen verhältnismäßige Eingriffsregelungen zu schaffen, wurden von der Bundesregierung nicht beachtet. In ihrem Gesetzentwurf vom 27. April 2007 wird demgegenüber der Schutz der Zeugnisverweigerungsberechtigten verringert, Benachrichtigungspflichten gegenüber betroffenen Personen werden aufgeweicht, Voraussetzungen für die Erhebung von Standortdaten in Echtzeit und für den Einsatz des IMSI-Catchers erheblich ausgeweitet und die Verwendungszwecke für die auf Vorrat gespeicherten Daten über die europarechtlichen Vorgaben hinaus auch auf leichte Straftaten, auf Zwecke der Gefahrenabwehr und sogar der Nachrichtendienste erstreckt.

Die nun im Bundesratsverfahren erhobenen zusätzlichen Forderungen zeugen von mangelndem Respekt vor den Freiheitsrechten der Bürgerinnen und Bürger. Dies zeigen folgende Beispiele: Die ohnehin überzogene Speicherdauer aller Verkehrsdaten wird von 6 auf 12 Monate verlängert. Die Überwachungsintensität erhöht sich durch eine Verschärfung der Prüfpflichten der Telekommunikationsunternehmen – bis zum Erfordernis des Ablichtens und Aufbewahrens von Identitätsnachweisen aller Personen, die Prepaid-Produkte nutzen wollen. Die Sicherheitsbehörden erhalten Auskunft über Personen, die bestimmte dynamische IP-Adressen nutzen. Ausschüsse des Bundesrates wollen die Nutzung dieser Daten sogar zur zivilrechtlichen Durchsetzung der Rechte an geistigem Eigentum gestatten und bewegen sich damit weit jenseits des durch die EG-Richtlinie zur Vorratsspeicherung abgesteckten Rahmens, die Nutzung auf die Verfolgung schwerer Straftaten zu beschränken. Weiterhin ist eine Ausdehnung der Auswertung von Funkzellendaten von Mobiltelefonen mit dem Ziel der Ermittlung des Aufenthaltes von möglichen Zeuginnen und Zeugen geplant. Daten, die Beweiserhebungs- oder verwertungsverboten unterliegen, sollen nicht unmittelbar gelöscht, sondern nur gesperrt werden.

Ganz nebenbei will der Innenausschuss des Bundesrats eine Rechtsgrundlage für die heimliche Online-Durchsuchung von Internet-Computern schaffen. Allein die Zulassung dieser Maßnahme würde rechtsstaatlichen Grundsätzen eklatant widersprechen und das Vertrauen in die Sicherheit der Informationstechnik massiv beschädigen.

Das Bundesverfassungsgericht hat in letzter Zeit eine Reihe von Sicherheitsgesetzen mit heimlichen Erhebungsmaßnahmen aufgehoben. Auch europäische Gerichte haben Sicherheitsmaßnahmen für rechtswidrig erklärt. Eine Entscheidung des Europäischen Gerichtshofs über die Verpflichtung zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten sollte abgewartet werden ebenso wie die Entscheidung des Bundesverfassungsgerichtes zur nordrhein-westfälischen Regelung, die dem Verfassungsschutz die Online-Durchsuchung erlaubt.

Die Forderungen im Gesetzgebungsverfahren zeugen von einem überzogenen Sicherheitsdenken. Sie führen dazu, dass die Freiheitsrechte der Bevölkerung untergraben werden. Sicherheit in der Informationsgesellschaft ist nicht mit überbordenden Überwachungsregelungen zu erreichen, sondern nur durch maßvolle Eingriffsbefugnisse mit effektiven grundrechtssichernden Verfahrensregelungen und durch deren besonnene Anwendung. Die betroffenen Grundrechte verkörpern einen zu hohen Wert, als dass sie kurzfristigen Sicherheitsüberlegungen geopfert werden dürfen.

21.8 Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring: Nachbesserung bei Auskunfteienregelungen gefordert

(Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2007)

Die fortschreitende technologische Entwicklung führt zu immer weitreichenderer Erfassung und Verknüpfung von persönlichen Daten und ermöglicht deren Auswertung für Kontroll- und Präventionszwecke. In der Privatwirtschaft ist daher ein engmaschiges Netz verschiedener Auskunftssysteme und branchenübergreifender Zentraldateien entstanden, die durch Profilbildung das Verhalten eines jeden Menschen ohne dessen Wissen und Wollen abbilden und bewerten können.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass das Bundesministerium des Innern endlich damit begonnen hat, die gesetzlichen Regelungen zu den Auskunfteien zu überarbeiten und neue Regelungen zum Scoring zu schaffen.

Die vorgesehenen Regelungen zu den Auskunfteien verschlechtern die Rechtsposition der Betroffenen. Sie tragen dem sich ständig weiter entwickelnden Auskunfteimarkt und den dadurch hervorgerufenen Bedrohungen für das Recht auf informationelle Selbstbestimmung nicht hinreichend Rechnung. Ziel einer gesetzlichen Regelung muss es sein, den rasant wachsenden, branchenübergreifenden Datenaustausch zu beschränken. Es kann nicht hingenommen werden, dass Auskunfteidienste nur einseitig das Informationsinteresse der angeschlossenen Unternehmen bedienen. Sie müssen auch in stärkerem Maße die schutzwürdigen Belange der betroffenen Bürgerinnen und Bürgern berücksichtigen. Mit der im Entwurf vorgesehenen Möglichkeit, die Auskunftstätigkeit auf jegliche rechtliche und wirtschaftliche Risiken zu erstrecken, wäre zu befürchten, dass letztlich bei allen vertraglichen Beziehungen – also auch bei Versicherungs- und Arbeitsverträgen – vorab Auskunfteien eingeschaltet werden. Damit würden die allgemeinen Vertragsrisiken im Wirtschaftsleben in nicht mehr angemessener Weise einseitig auf die Kundinnen und Kunden verlagert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber auf, die Situation der Verbraucherinnen und Verbraucher deutlich zu verbessern und mit dem Gesetzesvorhaben einen fairen Ausgleich zwischen den Interessen der Wirtschaft und der betroffenen Verbraucherinnen und Verbraucher zu schaffen. Die Konferenz hält es für dringend erforderlich, die Auskunfteitätigkeit auf kreditorische Risiken zu begrenzen. Zudem fordert die Konferenz, Auskunfteidienste branchenspezifisch zu begrenzen.

Der vorgelegte Referentenentwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes sieht beim Scoring nun Ansätze für ein transparenteres Verfahren für die Betroffenen vor. Es muss jedoch darauf geachtet werden, dass dieser Ansatz auch vorbehaltlos umgesetzt wird. Das Scoring, bei dem mittels einer mathematisch-statistischen Formel das zukünftige vertragstreue Verhalten eines Menschen durch einen Zahlenwert ausgedrückt wird, dringt seit Jahren in immer mehr Bereiche des Wirtschaftslebens vor. Den Betroffenen wurde jedoch bisher das Wissen darüber, wie sich der Scorewert zusammensetzt, vorenthalten. Diese Praxis soll der Gesetzentwurf beenden. Die Betroffenen sollen Auskunft darüber erhalten, welche Daten mit welcher Gewichtung in den jeweiligen Scorewert eingeflossen sind. Die vorgeschlagenen Regelungen gehen jedoch noch nicht weit genug.

Unbedingt zu streichen ist etwa eine im Entwurf enthaltene Regelung, wonach die Auskunft mit der Begründung verweigert werden kann, es würden Geschäftsgeheimnisse offenbart.

21.9 Nein zur Online-Durchsuchung

(Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2007)

Der Computer hat im täglichen Leben der meisten Menschen eine zentrale Bedeutung für die Aufbewahrung und Gestaltung privatester Informationen, wie Fotografien, Reiseberichte, Tagebuchaufzeichnungen, persönliche Briefe, Eindrücke, Vorstellungen und Gefühle. Die heimliche Online-Durchsuchung führt deshalb zu erheblichen Eingriffen in Grundrechte (informationelles Selbstbestimmungsrecht, Unverletzlichkeit der Wohnung, Telekommunikationsgeheimnis usw.). Die Installation von Überwachungssoftware etwa mit Hilfe des Internets oder die Versendung von E-Mails unter dem Namen einer anderen Behörde wird erwogen, sogar das unbemerkte Eindringen in Wohnungen zu diesem Zweck wird nicht ausgeschlossen.

Bei dem geforderten heimlichen Zugriff auf informationstechnische Systeme geht es nicht nur um „Online-Durchsicht“ als einmalige Durchsuchung und die damit verbundene Übertragung von Festplatteninhalten an die Strafverfolgungs- oder Sicherheitsbehörden, sondern auch um die anhaltende Überwachung, um das Ausspähen von Passworten und die Protokollierung aller elektronischen Aktivitäten. Auch sollen andere Kommunikations- und Datenverarbeitungssysteme, wie Computernetze, Mobiltelefone, PDA usw., in die heimliche Durchsuchung einbezogen werden. Dabei ist die Feststellung des Computers einer Zielperson technisch ohne Zusatzinformationen nicht ohne Weiteres möglich. Die Gefahr ist daher sehr groß, dass von einer solchen Maßnahme eine Vielzahl von – auch unverdächtigen – Nutzerinnen und Nutzern betroffen sein werden.

Es steht fest, dass sich der unantastbare Kernbereich privater Lebensgestaltung bei Online-Durchsuchungen durch technische Mittel bei der Datenerhebung nicht schützen lässt. Ein automatisierter Kernbereichsschutz ist somit nicht realisierbar.

Darüber hinaus wird eingeräumt, dass sich mit Hilfe der entsprechenden Software die auf den Festplatten gespeicherten Inhalte manipulieren ließen, was die Beweiseignung der gewonnenen Erkenntnisse und damit – jedenfalls bei der Verfolgung von Straftaten – die Geeignetheit der Online-Durchsuchung in Frage stellt.

Derzeit wird zwar versichert, dass der Einsatz nur auf die Bekämpfung des Terrorismus sowie die Verfolgung schwerster Straftaten und insgesamt auf wenige Fälle beschränkt wird. Die Erfahrungen zeigen aber, dass solche Beschränkungen nicht von langer Dauer sein werden. So begründen z.B. die drohende Aufweichung der Zweckbindung der Mautdaten und die Entwicklung der Telekommunikationsüberwachung die Befürchtung, dass Online-Durchsuchungen entsprechend dem technischen Fortschritt als Standardmaßnahme künftig auch bei Gefahren und Straftaten von geringerer Bedeutung eingesetzt werden. Zudem ist davon auszugehen, dass Terrorverdächtige Mittel und Wege finden werden, durch geeignete Gegenmaßnahmen eine erfolgreiche Online-Durchsuchung zu verhindern. Die heimliche Online-Durchsuchung führt deshalb voraussichtlich nicht zu mehr Sicherheit, aber sicher zur Einschränkung der Freiheit.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen daher ihre im Rahmen der 73. Konferenz im März 2007 erhobene Forderung an die Bundesregierung, die Landesregierungen

und die Parlamente, auf die Einführung der repressiven und präventiven Online-Durchsuchung zu verzichten.

Sie halten es für zwingend notwendig, dass das Urteil des Bundesverfassungsgerichts in dem Verfahren gegen die Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalens abgewartet wird.

21.10 Zentrale Steuerdatei droht zum Datenmoloch zu werden

(Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2007)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für inakzeptabel, dass die Bundesregierung mit dem Jahressteuergesetz 2008 im Schnelldurchgang ohne ausführliche parlamentarische Beratung die beim Bundeszentralamt für Steuern aufzubauende zentrale Steuerdatei um zusätzliche - teilweise sensible - Daten anreichern will. Zugleich droht die Steueridentifikationsnummer (Steuer-ID) bereits vor ihrer endgültigen Einführung zu einem allgemeinen Personenkennzeichen zu werden.

Der Gesetzentwurf sieht die Ablösung des Lohnsteuerkartenverfahrens durch ein elektronisches Abrufverfahren (ElsterLohn II) ab 2011 vor. Bereits am 9. November 2007 soll das Gesetz abschließend im Bundestag beraten werden. Geplant ist unter anderem, die in Zusammenhang mit der seit dem 1. Juli 2007 vergebenen Steuer-ID errichtete Datenbank um weitere Daten zu ergänzen, etwa um die Religionszugehörigkeit, Ehepartner/Ehepartnerinnen/Kinder und deren Steuer-ID, dazu Angaben über Steuerklassen. Hierbei werden auch zahlreiche Datensätze auf Vorrat aufgenommen, da auch Personen betroffen sind, die (noch) keine Arbeitnehmer/Arbeitnehmerinnen sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert vom Bundestag und Bundesrat, dieses Vorhaben der Umstellung auf ein elektronisches Verfahren mit dem Jahressteuergesetz 2008 nicht zu beschließen. Folgende Punkte sind datenschutzrechtlich kritisch:

- Der durch die Vergabe der Steueridentifikationsnummer an alle Steuerpflichtigen und damit für alle Einwohnerinnen und Einwohner der Bundesrepublik entstehende Datenpool erhält eine neue Dimension. Zwar sind die Lohnsteuerabzugsmerkmale auch bisher auf der Lohnsteuerkarte vermerkt. Die Speicherung dieser Daten in einer zentralen Datenbank würde aber erhebliche datenschutzrechtliche Fragen aufwerfen. In den zentralen Datenbestand würden die Daten aller Personen mit Lohnsteuerkarten einfließen, also auch von solchen Personen, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Es ist zweifelhaft, ob die Aufnahme dieses Personenkreises dem Erforderlichkeitsgrundsatz entspricht. Nützlichkeitserwägungen sind für eine Datenhaltung auf Vorrat in keinem Fall ausreichend.
- Die Daten würden bundesweit annähernd vier Millionen Arbeitgebern zur Verfügung stehen. Als einzige Sicherung ist dabei vorgesehen, dass nur ein autorisierter Arbeitgeber die Lohnsteuerabzugsmerkmale abrufen kann. Klärungsbedürftig ist allerdings, wie dies sichergestellt werden kann. Zwar ist ein Authentifizierungsverfahren für den Arbeitgeber vorgesehen. Die Frage ist jedoch, ob damit tatsächlich eine rechtswidrige Informationsbeschaffung Dritter auszuschließen ist. Zumindest sollten die Daten aus der zentralen Datenbank nur unter Mitwirkung der Betroffenen abgerufen werden können.
- Die gesetzlich vorgeschriebene Evaluierung des Verfahrens (§ 87a Abs. 6 AO) ist noch nicht erfolgt. Gleichzeitig existieren bereits jetzt Bestrebungen, die Kommunikationsplattform „Elster“ für Nutzungen durch andere Verwaltungszweige zu öffnen (OpenElster). Dies aber bedeutete, dass damit die Steuer-ID auch für die Identitätsfeststellung bei steuerfremden Anwendungen herangezogen werden könnte, ohne damit der strikten Zweckbindung nach § 139b Abs. 5

Abgabenordnung zu rein steuerlichen Zwecken Rechnung zu tragen. Diese Zweckbindung kann nach § 139b Abs. 2 AO auch nicht durch die jeweilige Einwilligung der betroffenen Bürgerinnen und Bürger überwunden werden. Mit OpenElster sollen diese Vorkehrungen offenbar aufgeweicht werden, bevor die Steuer-ID überhaupt eingeführt wurde. Allein dies macht deutlich, dass jede Erweiterung des zentralen Datenbestandes kritisch hinterfragt werden muss.

Schließlich ist zu befürchten, dass die vorgesehene Erweiterung der Datenbank beim BZSt nicht den Schlusspunkt darstellt. Die im neuen Datenpool gespeicherten Daten wären auch für Sozialleistungsträger und Strafverfolgungsbehörden interessant. Es gibt zahlreiche Beispiele, dass Daten, die zunächst nur für einen engen Zweck gespeichert werden dürfen, später für viele andere Zwecke verwendet werden: Die für steuerliche Zwecke erhobenen Daten über Freistellungsaufträge werden mit den ebenfalls beim BZSt gespeicherten Daten der Empfänger von BaföG- und anderen Sozialleistungen abgeglichen. Die Mautdaten, die zunächst nur zur Mautberechnung erhoben wurden, sollen zukünftig auch zur Strafverfolgung verwendet werden. Der zunächst ausschließlich zur Terrorismusbekämpfung und der Bekämpfung der organisierten Kriminalität eingeführte Kontendatenabruf steht heute auch Finanzämtern und anderen Behörden wie z.B. der Bundesagentur für Arbeit über das BZSt offen. Das BZSt enthält so einen einzigartigen aktuellen Datenpool aller Bundesbürgerinnen und -bürger, der wesentliche Meldedaten, Bankkontenstammdaten und Steuerdaten zentral verknüpfen kann.

21.11 Zuverlässigkeitsüberprüfungen bei Großveranstaltungen

(Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2007)

Anlässlich der Fußball-WM 2006 wurden im Rahmen der Akkreditierung umfassende Zuverlässigkeitsüberprüfungen nach einem auf Verwaltungsebene festgelegten Verfahren durchgeführt. Dabei wurde auf die Datenbestände der Polizei- und Verfassungsschutzbehörden des Bundes und der Länder zurückgegriffen. Dieses gesetzlich nicht vorgesehene Verfahren soll nunmehr beliebigen weiteren Veranstaltungen als Vorbild dienen.

Solche Zuverlässigkeitsüberprüfungen greifen in das Grundrecht auf informationelle Selbstbestimmung ein. Grundrechtseingriffe dürfen nicht unter Umgehung gesetzlicher Vorschriften durchgeführt werden, die Voraussetzungen und Begrenzungen solcher Verfahren regeln. Die Sicherheitsüberprüfungsgesetze des Bundes und der Länder sind für die Durchführung von allgemeinen Zuverlässigkeitsprüfungen, z. B. anlässlich von Veranstaltungen, nicht einschlägig. Eine generelle rechtliche Grundlage für Zuverlässigkeitsüberprüfungen besteht außerhalb der spezialgesetzlichen Bestimmungen nicht.

Einwilligungen können – auch wenn die Betroffenen über die Umstände informiert wurden – diese Maßnahme alleine nicht legitimieren. Dies nicht nur deshalb, weil Betroffene oft Nachteile befürchten müssen, wenn sie die Einwilligung verweigern und insoweit eine echte Freiwilligkeit fehlt. Viele Regelungen zu Überprüfungsverfahren verlangen – zusätzlich – zu den materiellen und verfahrensrechtlichen Regelungen die Mitwirkung der betroffenen Personen in Form einer schriftlichen Erklärung bei der Einleitung einer solchen Überprüfung. Außerdem sollen die Vorschriften ein transparentes Verfahren gewährleisten, in dem u. a. die Rechte Betroffener geregelt sind, so etwa das Recht auf Auskunft oder Anhörung vor negativer Entscheidung. Diese flankierenden Schutzmechanismen sind bei Überprüfungsverfahren unerlässlich.

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

22.1 Internationaler Datenverkehr

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 19./20. April 2007 in Hamburg)

1. Der Düsseldorfer Kreis beschließt das anliegende Positionspapier zum internationalen Datenverkehr. Der BlnBDI wird gebeten, das Papier als Vorsitzender der AG „Internationaler Datenverkehr“ an die damals beteiligten Wirtschaftsvertreter zu versenden, die zugleich darauf hingewiesen werden sollen, dass weitere Fallkonstellationen in einer allgemein zugänglichen Handreichung näher dargestellt werden.

Die im Positionspapier genannten Auffassungen können von den Aufsichtsbehörden bei der Beratung auch anderer Wirtschaftsvertreter genutzt werden.

2. Der Düsseldorfer Kreis beschließt ferner die anliegende Handreichung zur rechtlichen Bewertung von Fallgruppen zur internationalen Auftragsdatenverarbeitung. Sie beinhaltet die häufigsten Fallkonstellationen und soll den Unternehmen die rechtliche Bewertung erleichtern. Im Einzelfall kann eine abweichende Bewertung erforderlich sein. Deshalb verbieten sich schematische Lösungen. Den Aufsichtsbehörden wird anheim gestellt, die Handreichung im Internet zu veröffentlichen oder auf andere Weise interessierten Unternehmen zugänglich zu machen.

Die im Beschluss genannten Anlagen (Positionspapier und Handreichung) sind zu finden auf der Homepage des BfDI unter www.bfdi.bund.de unter Entschließungen des Düsseldorfer Kreises.

22.2 Kreditscoring / Basel II

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 19./20. April 2007in Hamburg)

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich beurteilen die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten beim Einsatz von Scoring-Verfahren im Bereich der Kreditwirtschaft wie folgt:

I. Welche personenbezogenen Merkmale dürfen für die Berechnung des Scores genutzt werden?

1. Es dürfen nur Parameter genutzt werden, deren Bonitätsrelevanz mittels eines den wissenschaftlichen Standards entsprechenden mathematisch-statistischen Verfahrens nachgewiesen wurde. Die statistische Relevanz eines Parameters ist für die Einstellung in das Scoring-Verfahren eine notwendige, aber noch keine hinreichende Bedingung.

2. Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG dürfen nur Daten erhoben und gespeichert werden, soweit dies zur Zweckbestimmung eines Vertragsverhältnisses erforderlich ist. Die Tatsache, dass ein Scoring-Verfahren durchgeführt wird, ändert daran nichts und erweitert nicht den Berechtigungsrahmen der Banken. Es dürfen daher nur Daten in ein Scoring-Verfahren eingestellt werden, die das Institut im Rahmen eines Kreditvertrages erheben darf (Erforderlichkeitsprinzip). Soweit Daten für andere Zwecke, etwa aufgrund von Vorgaben des KWG oder des WpHG erhoben und gespeichert wurden, dürfen diese Daten nur für diese Zwecke, nicht jedoch für Scoring-Verfahren verwendet werden. (Da sensitive Daten im Sinne des § 3 Abs. 9 BDSG nicht nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG erhoben und verarbeitet werden, dürfen diese auch nicht in die Score-Berechnung einfließen.)

3. Das Scoring-Verfahren selbst stellt eine Datennutzung dar. Für diese gilt § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Danach ist die Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Ein berechtigtes Interesse der Banken an der Nutzung der für das Scoring-Verfahren verwendeten Parameter kann in der Regel angenommen werden. Wenn das Kreditinstitut die Möglichkeit hat, konkrete, unmittelbar bonitätsrelevante Daten zu erheben, darf es nicht auf Daten zurückgreifen, die nur Indizcharakter haben.

Soweit ein berechtigtes Interesse der Banken vorliegt, ist bei jedem einzelnen Parameter zu überprüfen, ob der Betroffene überwiegende schutzwürdige Interessen am Ausschluss der Datennutzung geltend machen kann. Die hier vorzunehmende Abwägung stellt einen normativen Prozess dar; die bloße statistische Relevanz eines Kriteriums führt noch nicht dazu, dass nicht von überwiegenden schutzwürdigen Interessen des Betroffenen auszugehen ist.

Bei der Abwägung können die gesetzgeberischen Wertungen aus § 10 Abs. 1 Satz 3 ff. KWG herangezogen werden. § 10 Abs. 1 KWG gilt zwar als bankenaufsichtsrechtliche Norm nur für die Erhebung und Verarbeitung personenbezogener Daten zur internen Risikobemessung (Eigenkapitalausstattung), nicht jedoch für das Scoring im Außenverhältnis zu den (potentiellen) Kundinnen und Kunden. Die Wertungen aus § 10 Abs. 1 Satz 3 ff. KWG können allerdings als gesetzgeberisches Leitbild in die Auslegung des BDSG einfließen. Das gilt insbesondere für die

Anforderungen an Scoring-Merkmale. Die Merkmale müssen daher nicht nur mathematisch-statistisch erheblich sein, sondern eine ebenso hohe Stringenz aufweisen wie die im Merkmalskatalog des § 10 Abs. 1 Satz 6 KWG aufgeführten Regelbeispiele. So sind Angaben zur Staatsangehörigkeit bereits aufgrund des ausdrücklichen Verbots in § 10 Abs. 1 Satz 3 KWG als Score-Merkmale ausgeschlossen.

Bei der Abwägung sind darüber hinaus Wertungen des Grundgesetzes wie auch des einfachen Rechts daraufhin zu überprüfen, ob eine Benachteiligung der (potentiellen) Kundinnen und Kunden aufgrund eines bestimmten Kriteriums unzumutbar ist.

4. Auch wenn sich Basel II vornehmlich mit der Eigenkapitalhinterlegung der Institute befasst, wird der Einsatz von Scoring-Verfahren zunehmend dazu führen, jeden Kredit entsprechend dem individuellen Risiko zu bezinsen. Nur wenn in einer Gesamtschau der Kriterien sichergestellt ist, dass diesem Anliegen Rechnung getragen wurde, erfolgt die Datennutzung zur Wahrung berechtigter Interessen und sind keine überwiegenden schutzwürdigen Interessen der Betroffenen tangiert.

II. Wie transparent müssen die Bewertungen für die Betroffenen sein?

Für die Betroffenen (wie auch für die Aufsichtsbehörden) muss nachvollziehbar sein,

1. welche personenbezogenen Merkmale in die Berechnung des Score-Wertes einfließen;
2. welche konkreten personenbezogenen Daten der kreditsuchenden Person dafür genutzt wurden;
3. welches die maßgeblichen Merkmale sind, die den konkreten Score-Wert der betroffenen Person negativ beeinflusst haben. Diese maßgeblichen Merkmale sollen nach ihrer Bedeutung bzw. den Grad ihres Einflusses auf den konkreten Score-Wert aufgelistet werden, wobei sich die Auflistung auf die vier bedeutsamsten Merkmale beschränken soll.

Darüber hinaus ist bei der Anwendung von Scoring-Verfahren der § 6a BDSG zu beachten.

22.3 Mahnung durch Computeranruf

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 19./20. April 2007 in Hamburg)

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen dazu fest:

Eine telefonische Mahnung durch Computeranruf ist wegen der hohen Gefahr, dass ein anderer als der vorgesehene Empfänger die Nachricht erhält und so personenbezogene Daten einem Dritten unbefugt offenbart werden, unzulässig.

22.4 Erhebung von Positivdaten zu Privatpersonen bei Auskunfteien

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 19./20. April 2007 in Hamburg)

Nicht nur sog. Verbraucherauskunfteien wie beispielsweise die SCHUFA, sondern auch Handels- und Wirtschaftauskunfteien erheben und verarbeiten zunehmend Bonitätsdaten zu Privatpersonen, die nicht gewerblich tätig sind. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass die Handels- und Wirtschaftsauskunfteien insoweit die selben datenschutzrechtlichen Vorgaben zu beachten haben wie die "Verbraucherauskunfteien".

Handels- und Wirtschaftsauskunfteien können daher sog. Positivdaten zu Privatpersonen grundsätzlich nicht auf Grundlage des § 29 Abs. 1 BDSG erheben. Denn bei Positivdaten - das sind Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten zum Inhalt haben - überwiegt das schutzwürdige Interesse der betroffenen Personen, selbst über die Verwendung ihrer Daten zu bestimmen. Werden die Daten übermittelt, ist insoweit bereits die Übermittlung nach § 28 BDSG regelmäßig unzulässig.

Will eine Auskunftei Positivdaten zu Privatpersonen erheben, bedarf es dafür einer wirksamen Einwilligung der Betroffenen im Sinne des § 4a BDSG. Sofern die Auskunftei oder ihre Vertragspartner zu diesem Zweck eine für eine Vielzahl von Fällen vorformulierte Einwilligungsklausel verwenden, die als Allgemeine Geschäftsbedingung im Sinne des § 305 BGB zu werten ist, muss eine entsprechende Einwilligung darüber hinaus den Anforderungen des § 307 BGB genügen.

22.5 Weitergabe von umzugsbedingten Adressänderungen durch Versandhandelsunternehmen

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 19./20. April 2007 in Hamburg)

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen dazu fest: Übermittelt ein Unternehmen Umzugsadressen seiner Kunden an die Deutsche Post Adress GmbH zur weiteren Übermittlung an angeschlossene Unternehmen, so ist dies nur mit einer ausdrücklichen Einwilligung der Betroffenen gemäß § 4a BDSG zulässig.

Ein Datenschutzhinweis in den Allgemeinen Geschäftsbedingungen eines Versandhandelsunternehmens entspricht weder der Form noch dem Inhalt nach den Anforderungen an eine wirksame Einwilligung im Sinne von § 4a BDSG. Eine Einwilligung der Kunden setzt voraus, dass diese ausdrücklich darauf hingewiesen werden, welche Daten zu welchem Zweck an wen weitergegeben werden sollen.

22.6 Weitergabe von Kundendaten durch Versandhandelsunternehmen an Auskunfteien

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 19./20. April 2007 in Hamburg)

Die Übermittlung von personenbezogenen Daten über das vertragsgemäße Zahlungs- und Geschäftsabwicklungsverhalten ihrer Kunden sowie die Übermittlung von Scorewerten, die auf der Grundlage dieses Verhaltens berechnet wurden, durch Versandhandelsunternehmen an Auskunfteien zur Nutzung für deren eigene Geschäftszwecke ist unzulässig, es sei denn, die Kunden haben ausdrücklich in die Weitergabe dieser Daten eingewilligt.

Ein Datenschutzhinweis in den Allgemeinen Geschäftsbedingungen eines Versandhandelsunternehmens entspricht weder der Form noch dem Inhalt nach den Anforderungen an eine wirksame Einwilligung im Sinne von § 4a BDSG. Eine Einwilligung der Kunden setzt voraus, dass diese ausdrücklich darauf hingewiesen werden, welche Daten zu welchem Zweck an wen weitergegeben werden sollen.

Die Zulässigkeit einer Weitergabe von Kundendaten in dem genannten Umfang kann nicht auf § 28 BDSG gestützt werden, da sie nicht der Zweckbestimmung des Vertragsverhältnisses des Versandhandelsunternehmens mit dem Kunden dient (§ 28 Abs. 1 Satz 1. Nr. 1 BDSG) und die schutzwürdigen Interessen der Kunden an dem Ausschluss der Weitergabe ihrer Daten an Auskunfteien überwiegen (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG). Die Kunden, die im Versandhandel bestellen, müssen nicht damit rechnen, dass ihr bisheriges Kundenverhalten gegenüber einem Versandhaus entscheidend dafür sein kann, ob sie Lieferungen von anderen Unternehmen erhalten, die bei einer Auskunftei Bonitätsauskünfte einholen. Die Kunden dürfen nicht zum Objekt wirtschaftlichen Handelns dadurch gemacht werden, dass der Handel selbst definiert, was für die Kunden bzw. ihre Daten gut ist. Sie haben daher ein überwiegendes schutzwürdiges Interesse an dem Ausschluss der Vermarktung ihrer positiven Bonitätsdaten.

22.7 Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 8./9. November 2007 in Hamburg)

Im modernen Wirtschaftsleben kommt Auskunfteien eine ständig wachsende Bedeutung zu. Diese sammeln eine Vielzahl von persönlichen Daten auch über Privatpersonen, um sie Dritten insbesondere für die Beurteilung der Kreditwürdigkeit ihrer Geschäftspartner gegen Entgelt zur Verfügung zu stellen.

Während in der Vergangenheit vor allem Kreditinstitute, der Versandhandel und Telekommunikationsunternehmen Auskünfte abgefragt haben, werden Informationen zur Beurteilung der Kreditwürdigkeit zunehmend auch von Vermietern, Versicherungen und sonstigen Unternehmen eingeholt. Von den Auskunfteien wird dabei vielfach ein so genannter Scorewert übermittelt. Hierbei handelt es sich um einen Wert, der auf der Grundlage eines mathematisch-statistischen Verfahrens aus den bei der Auskunftei vorhandenen Angaben errechnet wird und eine Aussage über die Wahrscheinlichkeit des künftigen Zahlungsverhaltens der Betroffenen und damit über ihre Kreditwürdigkeit enthält.

Der Aufbau und die Erweiterung der zentralen Datenbestände über Betroffene bei Auskunfteien und die branchenübergreifende Bereitstellung dieser Informationen für eine Vielzahl von Unternehmen sowie der zunehmende Einsatz von Scoring-Verfahren gefährden nachhaltig das Recht auf informationelle Selbstbestimmung der Betroffenen.

Vor diesem Hintergrund begrüßt der Düsseldorfer Kreis im Grundsatz den vom Bundesministerium des Innern vorgelegten Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes, mit dem die Rechte der Betroffenen gestärkt und insbesondere auch die Transparenz beim Einsatz von Scoring-Verfahren verbessert werden sollen.

Nach Auffassung des Düsseldorfer Kreises bedarf der vorliegende Gesetzentwurf allerdings einer grundlegenden Überarbeitung, um das Ziel der Stärkung der Rechte der Betroffenen auch tatsächlich zu erreichen.

Dabei muss insbesondere sichergestellt werden, dass die bei Auskunfteien gesammelten Daten die Erstellung umfassender Persönlichkeitsprofile von Betroffenen nicht zulassen. Darüber hinaus ist gesetzlich eindeutig zu regeln, dass die Einholung einer Bonitätsauskunft auch in Zukunft an das Vorliegen eines finanziellen Ausfallrisikos geknüpft bleibt. Die im Entwurf derzeit vorgesehene Regelung, wonach jedes rechtliche oder wirtschaftliche Interesse einschließlich der Vermeidung allgemeiner Vertragsrisiken ein berechtigtes Interesse darstellen kann, würde die Rechte der Betroffenen unverhältnismäßig beeinträchtigen.

Des Weiteren muss eindeutig klargestellt werden, dass nur vertragsrelevante Daten in die Berechnung eines Scorewerts einbezogen werden dürfen. Im Übrigen dürfen die Auskunftsrechte der Betroffenen nicht durch die pauschale Berufung auf ein Geschäftsgeheimnis vereitelt werden.

22.8 Anwendbarkeit des Bundesdatenschutzgesetzes auf Rechtsanwälte

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 8./9. November 2007 in Hamburg)

Der Düsseldorfer Kreis begrüßt, dass die Bundesregierung in ihrer Stellungnahme zum 21. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erklärt hat, dass die Erhebung und Verwendung personenbezogener – auch mandatsbezogener – Daten durch Rechtsanwälte den Vorschriften des Bundesdatenschutzgesetzes unterliegt und dass die Aufsichtsbehörden der Länder zuständig sind, die Datenschutzkontrolle durchzuführen.

Der Düsseldorfer Kreis sieht darin die Bestätigung seiner Auffassung, dass das Bundesdatenschutzgesetz (BDSG) – auch hinsichtlich mandatsbezogener Daten – auf Rechtsanwälte anwendbar ist. In der Bundesrechtsanwaltsordnung (BRAO) befinden sich aus datenschutzrechtlicher Hinsicht nur punktuelle Regelungen (§ 43a Abs. 2 BRAO Schweigepflicht, § 50 BRAO Handakten). Die Vorschriften des BDSG treten gemäß § 1 Abs. 3 BDSG lediglich insoweit zurück, als bereichsspezifische Datenschutzvorschriften bestehen. Durch das anwaltliche Berufsgeheimnis werden die In-formationsrechte der Aufsichtsbehörden nach § 38 BDSG in Verbindung mit § 24 Abs. 6 und 2 BDSG nicht eingeschränkt.

23. Die Europäische und die Internationale Datenschutzkonferenz

Die Europäische Konferenz und die Internationale Konferenz der Datenschutzbeauftragten, an denen ich nicht teilnahm, haben eine Reihe wichtiger Entschließungen gefasst, deren Abdruck allerdings den Rahmen des Jahresberichts sprengen würde. Ich bescheide mich daher, an dieser Stelle nur auf die Themen der Beschlüsse und Entschließungen hinzuweisen.

Entschließungen der Europäischen Datenschutzkonferenz:

11. Mai 2007

- Beschlüsse der Europäischen Datenschutzkonferenz Zypern 10. - 11. Mai 2007
- Erklärung von Zypern
- Entscheidung der Europäischen Datenschutzkonferenz über die Zukunft der Arbeitsgruppe Polizei (PWP)
- Erklärung zum gemeinsamen Standpunkt der Europäischen Datenschutzkonferenz über die Anwendung des Verfügbarkeitsprinzips bei der Strafverfolgung

Entschließungen der Internationalen Datenschutzkonferenz:

29. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre am 28. September 2007

- Akkreditierungsbeschluss
- Resolution über den dringenden Bedarf an globalen Standards zum Schutz von Passagierdaten, die von Regierungsstellen zu Justizvollzugs- und Grenzschutzzwecken herangezogen werden
- Resolution über die Entwicklung internationaler Standards
- Resolution über internationale Zusammenarbeit

Die Inhalte der hier aufgeführten Beschlüsse/Entschließungen stehen u. a. auf der Internetseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter

http://www.bfdi.bund.de/cln_007/nn_533554/DE/Oeffentlichkeitsarbeit/Entschliessungssammlung/Entschliessungen__node.html__nnn=true

zur Verfügung.

24. Anhang

24.1 Auswahl der Medienberichte in Tageszeitungen/Zeitschriften im Jahr 2007 mit Themen aus dem Land Bremen

Datum	Zeitung	Titel/Inhalt
02.01.2007	Bremer Tageszeitungen	**Sensible Daten nicht mehr per Post** BAgIS reagierte auf Einwand einer betroffenen Kundin
10.01.2007	Bremer Tageszeitungen	**79,99 Dollar verraten die Pädophilen** Technische Dienstleister der Banken entlarvten Käufer von Kinderpornografie
19.01.2007	Bremer Tageszeitungen	**Dataport nimmt seine Arbeit in Bremen auf** Norddeutscher Verbund für öffentliche Auftraggeber eröffnet Filiale
30.01.2007	Bremer Tageszeitungen	**Das Thema: Datenschutz in der Defensive – Im Clinch mit USA um Datenschutz** „Manchmal geht der Staat zu weit“ Seit dem 11. September gerät Datenschutz unter Druck
06.02.2007	taz-nord-bremen	**Schutz in schlechter Verfassung** Verfassungsschutz-Mitarbeiter des Geheimnisverrats beschuldigt: weil er bekannt gab, der Amtsleiter müsse sich für „Mobbingattacken“ rechtfertigen. Der sieht „hervorragendes Betriebsklima“
06.02.2007	Bremer Tageszeitungen	**Das Thema: Streit um Pläne zur PC-Durchsuchung** **Heimliche Online-Durchsuchungen verboten** **Bei Klick ist die Privatsphäre dahin** Schlimmer als der Große Lauschangriff?
20.03.2007	Bremer Tageszeitungen	**Der Staat surft mit: Internet-Fahndung wird ausgeweitet** Koalitionsexperten bereits im Grundsatz einig: Online-Durchsuchungen beim Verdacht schwerster Verbrechen erlauben
20.03.2007	Bremer Tageszeitungen	**CeBIT: Hilft nur noch die Internet-Interpol?** Schadsoftware nimmt ständig zu
21.03.2007	Kreiszeitung Syke	**Bürgerservicekoffer im Weserpark** Innenressort und Stadtamt testen Pilotprojekt / Mobile Dienstleistungen
21.03.2007	Bremer Tageszeitungen	**Strenge Regeln für drogenabhängige Eltern** Senat will Voraussetzungen für Methadonvergabe vereinheitlichen
21.03.2007	Bremer Tageszeitungen	**Pauschale Videoüberwachung verletzt Grundrechte** Regensburg darf jüdisches Kunstwerk nicht ständig observieren
21.03.2007	Bremer Tageszeitungen	**Kommentar: Wachsames Auge** Verfassungsgericht stoppt Überwacher
22.03.2007	Bremer Tageszeitungen	**Gesetze auf dem Prüfstand** Auch Online-Durchsuchungen

22.03.2007	Bremer Tageszeitungen	**Lange gesucht und kaum etwas gefunden** Bremens Verfassungsschutz wusste wenig über Kurnaz, er hat ihn kurzerhand gefährlich „geschrieben“
22.03.2007	Bremer Tageszeitungen	**Zielfahndung, Streuschüsse oder ein BKA-Schleppnetz im Internet?** Die geplante Online-Durchsuchung: Traum für Ermittler und Alptraum für Bürgerrechtler, Datenschützer und Journalisten
22.03.2007	Focus online	**Behörde soll Bericht manipuliert haben** Der Bremer Verfassungsschutz soll einen Bericht über den früheren Guantanamo-Häftling Murat Kurnaz manipuliert haben
22.03.2007	Berliner Zeitung online	**Kurnaz über Monate observiert** Verfassungsschutz überwachte Türken länger als bekannt
22.03.2007	Berliner Zeitung online	**Kurnaz offenbar noch im Februar überwacht** Beobachtung womöglich im Zusammenhang mit BND-Ausschuss
22.03.2007	Bremer Tageszeitungen	**Amt manipulierte Kurnaz-Bericht** Untersuchungsausschuss befasst sich mit schweren Vorwürfen gegen Bremer Verfassungsschützer
23.03.2007	Radio Bremen	**Bremer Datenschutzbericht 2006 kritisierte unter anderem geplante „Online-Durchsuchungen“**
27.03.2007	Bremer Tageszeitungen	**Video-Urteil erfreut Datenschützer** Karlsruhe kippt Kameraüberwachung in Bayern / Restriktionen auch für andere Bundesländer
24.04.2007	Bremer Tageszeitungen	**Wahlwerbung in der Grauzone** Datenschützer haben Rechtsextremist Siegerist wegen Telefonaktion im Visier
25.04.2007	Bremer Tageszeitungen	**Datenschutzrecht hält nicht Schritt/Eine Rüge für den Datenschutz** Beauftragter Schaar: Staat vernachlässigt Grundrechte
25.04.2007	Das BLV	**Bald die „Totale Überwachung“?** Datenschutzexperte referierte auf Einladung der jungen Sozialisten
03.05.2007	taz-nord-bremen	**Kein Verlass auf Datenschutz** Künstlerin protestiert gegen die Ausschnüffelung der Privatsphäre durch B-Chips
15.05.2007	taz-nord-bremen	**Überwachung unerwünscht** Beschwerde der Datenschützer gegen Abtasten von Autokenn-zeichen
22.05.2007	Bremer Tageszeitungen	**Kritik an Überwachung** Grundrechte-Report 2007 vorgestellt
24.05.2007	taz-nord-bremen	**Studis unter Terrorverdacht** Bei der G 8-Razzia gegen einen Dozenten der Bremer Uni Beschlagnahme die Bundesanwaltschaft auch Teilnehmerlisten seiner Seminare – beste Voraussetzung, nun auch die Studis zu verdächtigen

31.05.2007	taz-nord-bremen	**Datensammlung gegen Mietnomaden** Eigentümer haben Angst vor zahlungsunfähigen Mietern, die Wohnungen mit offenen Rechnungen verlassen. Gefundenes Fressen für private Schuldnerkarteien: Sie sammeln sensible Infos über Bewerber und verkaufen sie. Mieterschützer besorgt.
02.06.2007	Bremer Tageszeitungen	**Freud und Leid als „0“ und „1“** Bremer Kliniken digitalisieren Patientenakten
20.06.2007	Bremer Tageszeitungen	**Datenschützer kritisieren Google** Suchmaschine speichert Recherchen 18 Monate / Benutzer-verhalten wird transparent
21.06.2007	Bremer Tageszeitungen	**Gewinnspiel: Datenschützer mahnt zur Vorsicht** Post sammelt Informationen für Marketing und Werbung / Landesbeauftragter meldet Bedenken an
04.07.2007	Bremer Tageszeitungen	**Kahn – „Frau im Spiegel“ 2:0** Auch Bundesgerichtshof untersagt Veröffentlichung von Fotos
05.07.2007	Radio Bremen Nachrichten	**Bremer Datenschützer warnt vor grenzenloser staatlicher Überwachung** Durch die bundesweite Einführung einer steuerlichern Identifikationsnummer wird momentan ein bundeseinheitliches zentralen Melderegisters aufgebaut
06.07.2007	taz-nord-bremen	**Orwell ante portas** (siehe vor)
16.07.2007	Bremer Tageszeitungen	**Köhler zweifelt an Schäubles Ideen** Bundespräsident kritisiert Vorschläge zur Terrorabwehr
16.07.2007	Bremer Tageszeitungen	**Schäuble denkt auch an den Todesschuss** Bundesinnenminister hat neue Vorschläge zur Terrorabwehr gemacht
17.07.2007	Bremer Tageszeitungen	**Mehr Polizei statt neuer Gesetze** Justizministerin Zypries kritisiert Unionsvorschläge zur Abwehr von Terrorgefahr
24.07.2007	Bremer Tageszeitungen	**Daten-Speicherung erlaubt** Terrorfahnder der USA dürfen die Daten europäischer Fluggäste künftig 15 Jahre lang speichern
27.07.2007	taz-nord-bremen	**Kommissarin Linnert** Antrittsbesuch der Senatskommissarin für den Datenschutz beim Landesbeauftragten für Datenschutz
27.07.2007	taz-nord-bremen	**Kommentar: Rückenwind für den Datenschutz**
08.08.2007	Radio Bremen Nachrichten	**Unterschiedliche Reaktionen auf elektronische Steuerkarte in Bremen und Niedersachsen**
14.08.2007	Nordsee-Zeitung	**Datenschützer rümpfen Nase über virtuellen Lohnnachweis**
30.08.2007	Bremer Tageszeitungen	**Trojaner entzweien Koalition** Details über geplante Online-Durchsuchung sorgen für heftigen Streit
30.08.2007	Bremer Tageszeitungen	**Erst Hausbesuch, dann Trojaner** Online-Spionage: Experten skeptisch
30.08.2007	Bremer Tageszeitungen	**Getarnte E-Mails sollen PC ausspähen** Online-Durchsuchung: Auch Handys in Schäubles Visier

30.08.2007	Bremer Tageszeitungen	**Kommentar: Schäuble geht zu weit**
06.09.2007	Kommune 21	**Digitale Fälle** Das Sozialamt in Bremerhaven arbeitet mit elektronsicher Aktenführung. Die Funktionen des Fachverfahrens wurden durch eine Schnittstelle zum DMS erheblich erweitert
12.09.2007	taz-nord-bremen	**Hürden höher hängen** Das Chaos Computer Club informiert über „Überwachung in der Informationsgesellschaft“
19.09.2007	Bremer Tageszeitungen	**Film ab bei der Bremer Polizei** Videoaufnahmen sollen Verkehrspolizisten schützen
19.09.2007	Nordsee-Zeitung	**Mehr Aggressionen bei Polizeikontrollen** Beamte schützen sich mit Videoaufnahmen
19.09.2007	taz-nord-bremen	**Bürger werden gefilmt** Neues Videoaufzeichnungssystem auch bei Bremer Polizei eingeführt. Datenschützer erhebt keine Bedenken
19.09.2007	Kreiszeitung Syke	**Auch der brave Bürger wird gefilmt** Verkehrskontrollen mit Videoüberwachung sollen Bremer Polizisten vor Übergriffen von Autofahrern bewahren
21.10.2007	Weser-Report	**Online-Jammerlappen für Lehrer** Verkehrte Welt im Internet: Jetzt erhalten Bremer Pauker Zeugnisse von ihren Schülern
26.10.2007	taz-nord-bremen	**Der Druck ist sofort da** Ab nächster Woche gibt es Pässe nur gegen Abgabe der Fingerabdrücke. Noch werden diese nicht zentral gespeichert. Doch ob das bei den neuen Personalausweisen auch so sein wird, weiß niemand
27.10.2007	Bremer Nachrichten	**Einsamer Rufer in der Wüste** Datenschützer schlagen Alarm
30.10.2007	Bremer Tageszeitungen	**„Weltherrschaft“ via Vista** Experten halten Microsofts neues Betriebssystem für indiskret
30.10.2007	Nordsee-Zeitung	**Beistand für gläserne Bürger** Grundrecht auf Datenschutz in der Landesverfassung besteht jetzt zehn Jahre
30.10.2007	Bremer Nachrichten	**Sicherheitspanne bei ebay**
02.11.2007	Bremer Nachrichten	**Fingerabdrücke im Chip gespeichert** Bundesregierung: Reisepass seit gestern fälschungssicher
02.11.2007	Bild-Bremen	**Erste Kamera auf der Discomeile**
02.11.2007	Bremer Tageszeitungen	**Ohne Fingerabdruck geht´s nicht mehr** Seit gestern gilt der neue E-Reisepass
02.11.2007	Bremer Nachrichten	**„Datenschutz leidet nicht“** Wolfgang Bosbach (CDU) über den neuen elektronischen Reisepass
02.11.2007	Bremer Nachrichten	**Kommentar: Angst hält sich in Grenzen** Die Angst vor dem gläsernen Bürger

10.11.2007	Bremer Tageszeitungen	**„Turbulente Zeiten für Datenschützer“** Landesbeauftragter Sven Holst über Verfassung, Vorratsdatenspeicherung und Videoüberwachung
14.11.2007	Burg-Lesumer-Vereinsblatt	**Landesdatenschutzbeauftragter nimmt Stellung zur Vorratsdatenspeicherung** „Die Bürger müssen sich weiterhin frei und unbeobachtet fühlen können“ DATENSPEICHERUNG – Der Bürger wird noch gläserner
15.11.2007	taz-nord-bremen	**Lauschangriff auf G8-Gegner** Bei den Hausdurchsuchungen von G8-Gegnern im Mai sind die Wohnungen verwanzt worden. Der Bundesgerichtshof zweifelt derzeit daran, ob die Maßnahmen nach dem Terrorparagrafen 129a überhaupt gerechtfertigt waren
27.11.2007	Bremer Tageszeitungen	**Jahrelang falsch behandelt?** Bremer Mediziner erhebt im Fall Klasnic massive Vorwürfe – auch gegen Werders Arzt
22.12.2007	Bremer Tageszeitungen	**Kamera filmt Flirts und Schlägereien** Seit gestern wird die Discomeile nachts videoüberwacht / Senator Lemke will eine „sichere Meile zum Feiern“
23.12.2007	taz-nord-bremen	**Party unter Beobachtung** Mit Videokameras filmt die Polizei ab diesem Wochenende das Treiben auf der Discomeile. Ob die Privatsphäre in Wohnungen mittels digitaler Verfremdung gewahrt bleibt, ist fraglich Kommentar: Kein Problem
27.12.2007	Bremer Nachrichten	**Köhler billigt Datenspeicherung**

Bremer Tageszeitungen = Weser Kurier und Bremer Nachrichten

24.2 Auswahl telefonischer Anfragen

Thema	Antragsteller/-in
Übermittlung Bank- und Dienstreisedaten an ein konzerneigenes Reisebüro zu Werbezwecken	Beschäftigte
Aufnahme von Unterlagen über die Gründe einer Kündigung in die Personalakte	Beschäftigter
Erteilung von Auskünften aus dem Einwohnermelderegister	Bürger
Abrufberechtigung im Gewerberegister	Behörde
Übermittlung von Mitgliedsdaten eines Sportvereins an Verband	Bürger
Übertragen von Rettungsdienstprotokolldaten an Kliniken	Behörde
Speicherung von Daten durch die SCHUFA	Bürgerin
Anforderung eines ärztlichen Gutachtens beim Vormundschaftsgericht durch die Rentenversicherung	Versicherte
Eintrag bei Auskunftei nach verweigerter Annahme einer Schlechtlieferung	Kunde
Auskunft aus dem Schuldnerverzeichnis	Bürgerin
Kopien von Personalausweisen durch Wachpersonal	Bürger
Übermittlung von Gesundheitsdaten an die Berufsgenossenschaft durch den Arbeitgeber	Beschäftigte
Einsicht in das E-Mail-Fach durch eine andere Person	Beschäftigte
Einbehalt der Kirchensteuer unter Inanspruchnahme von Kreditinstituten	Bürger
Bekanntgabe von Schülerdaten in der Zeugniskonferenz	Behörde
Entsorgung von Datenträgern	Behördlicher Beauftragter für Datenschutz
Speicherung von Daten durch eine Auskunftei	Bürger
Weitergabe von Daten durch die Stadtwerke	Bürger
Videoüberwachung eines Nachbargrundstücks	Nachbarn
Akteneinsicht beim Jugendamt	Beteiligter
Befragung in einer Schule zu Essstörungen	Schüler
Vorlagepflicht Personalausweis, Ordnungswidrigkeit	Bürger
Weitergabe von psychosozialen Gutachtendaten an Dritte	Mobbing-Geschädigte
Weitergabe von Sozialdaten an ein Meinungsforschungsinstitut durch die Agentur für Arbeit	Beschäftigte
Datenspeicherung durch Auskunfteien	Bürger
Datenerhebung bei Arbeitsunfähigkeit, Schule in Bremen	Beschäftigte
Videoüberwachung des Eingangs eines Mehrfamilienhauses	Bewohner, Besucher etc.
Bekanntgabe von Schulzensuren vor der Klasse durch die Lehrkraft	Schüler
Vorlage des Einkommenssteuerbescheides zur Berechnung des Krankenkassenbeitrages	freiwillig Krankenversicherte
Anfordern einer Einwilligung in Videoaufnahmen einer Therapie	ALG I-Bezieher
Einholen der Einwilligung für Lichtbildveröffentlichung im Intranet	Behörde
Rechtsschutz gegen erfolgte Durchsuchung, Beschlagnahme und TKÜ	Bürger

Heimliche Vaterschaftstest, informationelle Selbstbestimmung des Kindes	Bürger
Gestaltung einer Einwilligungsklausel für Werbezwecke	Unternehmen
Voraussetzungen für eine Videoüberwachung	Unternehmen
Datenschutzrechtliche Anforderungen beim Direktmarketing	Bürger
Personalausweis als Zwangspfand in Diskotheken	Bürger
Mitnahme von Akten aus der Behörde	Behörde
Einsicht in Betreuungsakten von Angehörigen	Bürger
Berichtigung von personenbezogenen Angaben in medizinischen Gutachten	Bürger
Weitergabe personenbezogener Daten durch Kindergartenleiterin	Bürgerin
Weitergabe von Patientendaten durch Psychotherapeuten an die Kassenärztliche Vereinigung um Zulassung zu erhalten	Bürger
Weitergabe von Sozialdaten an andere Behörden	Behörde
Auskunft über bei der Polizei gespeicherte personenbezogene Daten	Bürger
Konkurrenzsituation des § 29 VwVfG zum BremIFG	Bürger
Bestellung von Datenschutzbeauftragten und Ahndung von Verstößen gegen Datenschutzvorschriften	Beschäftigte, Bürger und Kunden
Entwicklung der DV-Systeme "Mobiles Stoß-Monitoring" und "Mobiles Schmerztagebuch" durch eine Computerfirma	Patienten
Melde-/Bestellpflicht nach dem BDSG	Unternehmen
"Internationales polizeiliches Führungszeugnis" für Visumserteilung	Bürger
Löschfristen bei Eintragungen von Jugendlichen im polizeilichen Informationssystem	Bürger
IT-Dienstleister zugleich externer DSB? Interessenkollision	Unternehmen
Löschfristen Auskunftei bei titulierter ausgeglichener Forderung	Bürger
Datenerhebung über Durchschnittsnoten ehemaliger Schüler	Schüler
Erhebung von Meldedaten von in Niedersachsen lebenden Frauen durch die Zentrale Stelle Mammographie	Frauen zwischen 50 und 69 Jahren
Nutzung des Online-Lernprogramms datenschutz4school	Beauftragter für Datenschutz
Zugriff des Stellvertreters eines Vorgesetzten auf Krankenzeiten im Mitarbeiterportal	krank gemeldete Beschäftigte
Veröffentlichung von Bilddaten im Internet und politischen Flyern	politischer Mitstreiter
Aufgaben des behördlichen Datenschutzbeauftragten	Gesellschaft
Akkreditierung von Mitarbeitern der Senatskanzlei	Mitarbeiterin
Weitergabe von polizeilichen Daten an die Öffentlichkeit	Betrieblicher Beauftragter für Datenschutz
Verwendung von personenbezogenen Daten aus Ausschussbericht	Bürger
Datenerhebungen der Fa. Lifestyle	Bürgerin
Bestellung eines betrieblichen Datenschutzbeauftragten	Unternehmen
Frage nach dem Leberwert eines ALG-II-Empfängers durch die BAgIS	ALG II-Empfänger
Befragung von Schülerin über die Kenntnis von Straftatbeständen	Schüler
Erhebung von Daten bei der Durchführung des Mikrozensus	Bürgerin
Forschung im Kindertagesstätten und Schulen	Kinder, Schüler und deren Eltern
Forschung mit Gesundheitsdaten	Patienten

Erteilung von Führungszeugnissen	Bürger
Einsicht in Gesundheitsakten der Bundeswehr	Bürger
Datenschutz bei Telekommunikationsanbieter	Bürgerin
Übermittlung von personenbezogenen Daten an Parteien	Bürgerin
Einsatz eines Intranets im Unternehmen	Beschäftigte
Bestellung eines betrieblichen/behördlichen Datenschutzbeauftragten	Museumsmitarbeiter
Berichtigung von Daten durch die SCHUFA	Bürger
Weitergabe von Daten der Einsatzleitstelle der Feuerwehr an Dritte	Betrieblicher Beauftragter für Datenschutz
Aufzeichnung von Telefongesprächen beim ärztlichen Notdienst	Patienten und Beschäftigte
Erhebung personenbezogener Daten bei der Abholung von Paketen	Bürger
Verpflichtung der Schüler zum Ausfüllen von Fragebogen im Rahmen einer Evaluierung durch eine Schule	Schüler
"Telefonische Wahlwerbung" durch Wahlkampfkandidaten	Mehrere Bürger und Bürgerinnen (ca. 15 Personen)
Herausgabe einer Videoaufzeichnung zur Verfolgung rechtlicher Ansprüche	Opfer und Beschuldigter
Auskunft personenbezogener Daten an die Polizei	Bürger
Vermeidung von Werbeanrufen per Telefon (Robinson-Liste)	Bürger
Aufzeichnung von personenbezogenen Daten beim Warenumtausch	Bürgerin
Datenaustausch bei Kundenbindungssystemen	Bürgerin
Akteneinsicht im Petitionsausschuss	Behörde
Erhebung von Daten über Familienangehörige im Bewerbungsverfahren	Bewerber
Datenweitergabe an Nachbarn durch eine Spedition	Bürgerin
Polizeiliches Führungszeugnis bei Wohnsitz im EU-Ausland	Bürger
Aufbewahrung einer Ausweiskopie	Bürgerin
Lesebestätigung ohne Einwilligung bei E-Mails	Bürger
Verschlusssachenanweisung der Freien Hansestadt Bremen	Behörde
Datenübermittlungen einer Auskunftei für Mieterdaten	Bürger
Datenerhebungen durch Auskunfteien	Bürger
Datenerhebungen eines Handelsunternehmens	Bürgerin
Maßnahmen gegen telefonische Werbeanrufe	Bürgerin
Auskunft zur Einholung eines polizeilichen Führungszeugnisses	Bürgerin
Datenspeicherung durch Rechenzentren	Bürger
Datenerhebungen durch die Polizei	Bürger
Datenübermittlung von Altersbezügen an BaföG-Stelle	Unternehmen
Videoüberwachung und Biometrie	Bürger
Datenübermittlung der Polizei an andere Behörden	Betrieblicher Beauftragter für Datenschutz
Wirksamkeit einer Einwilligung bei Telefonaufzeichnungen durch Kreditinstitut	Bürgerin
Akteneinsicht nach § 406e StPO	Bürger
Auskunftspflicht gegenüber dem StaLa (Microzensus)	Bürgerin

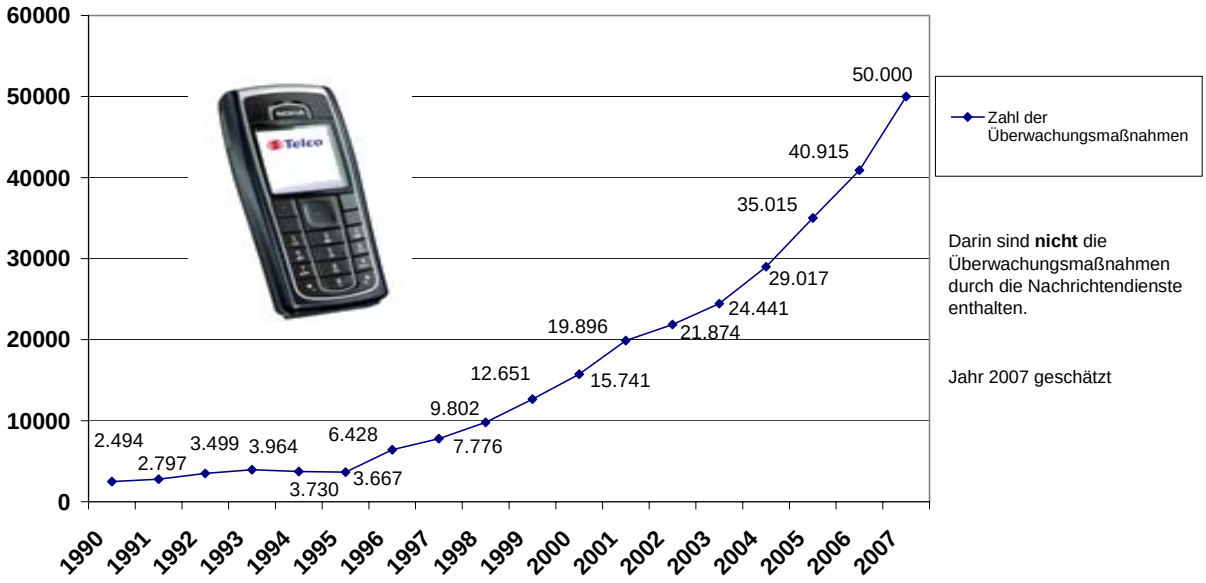
Impressumspflicht und Gestaltung bei Internetauftritt	Unternehmen
Sicheres Löschen von Daten bei kaputter Festplatte und Garantiefall	Bürger
Aufbau einer Datei über Frauen in Führungspersönlichkeiten durch die ZGF	Frauen in Führungspositionen
Aufnahme der privaten Handy-Nummern in eine Mitarbeiterdatenbank	Beschäftigte
Auskunft über die Herkunft von Daten bei einem Rechtsanwalt und Verletzung des Anwaltsgeheimnisses	Dritte und Prozessgegner
Datenerhebung beim Melderegister über die Wohnanschriften der letzten 30 Jahre durch einen Rechtsanwalt	Vermieter und Prozessgegner
Auskunft über den Score-Wert einer Auskunftei (Bremen)	Bürger
Videoüberwachung des Schulsekretariats	Beschäftigter und Besucher
Schullaufbahnakten in offenen Schränken, aber verschlossenen Räumen	Schüler
Weitergabe von Personalaktendaten an Dritten	Bürger
Anwendung kirchlichen Datenschutzrechts auf diakonische Einrichtungen	Bürger
Nutzung von Adressdaten für Marketingzwecke	Betrieblicher Beauftragter für Datenschutz
Erteilung von Auskünften zu Führungszeugnissen	Bürgerin
Einsicht in E-Mails durch Vorgesetzte und Kollegen	Beschäftigte
Zusendung von Telefonrechungen mehrerer Bundesbürger an einen Telefonkunden	Polizeibeamter
Einstellung einer Urlaubsliste ins Intranet und Einsicht durch alle Beschäftigten	Beschäftigte
Veröffentlichung eines Fotos und der Geburtsdaten in einer firmeninternen Hauszeitung	Beschäftigte
Beantragung eines polizeilichen Führungszeugnisses bei Wohnsitz in den Niederlanden	Bürgerin
Zugriff auf die privaten Telefonnummern der Beschäftigten durch alle anderen Beschäftigten	Beschäftigte
Vorlage des Personalausweises und Hinweis auf die Datenverarbeitung bei Schmuckverleihgeschäften	Kunden
Aufnahme der Privatanschrift auf Briefumschlägen mit Gehaltsabrechnungen trotz firmeninterner Verteilung	Beschäftigte
Weitergabe von Grundschulzeugnissen	Bürgerin
Jugendamtsakten im Internet	Bürger
Videoüberwachung im Dienstraum eines Altenpflegeheimes	Beschäftigte
Sicherheitsüberprüfung nach dem Atomgesetz	Bürger
Weitergabe von Bedienstetendaten im Rahmen einer Organisationsabfrage	Behörde
Videoüberwachung einer unter Denkmalschutz stehenden Brücke im Bürgerpark zur Verhütung von Graffiti	Parkbesucher
Weitergabe von Mieterdaten an eine Sozialeinrichtung durch den Vermieter	Mieter
Vorzeigen des Personalausweises beim Abholen von Fotos	Bürgerin
Telefonische Wahlwerbung von politischen Parteien	Bürgerin
Auskunft über bei der Polizei und dem LfV gesicherte Daten	Bürgerin
Mithören durch "Kaltanrufe" in Call Centern durch den Auftraggeber	Beschäftigte, Kunden
Weitergabe von Mieterdaten an die Mutter des Mieters wegen	Mieter

Zahlungsschwierigkeiten

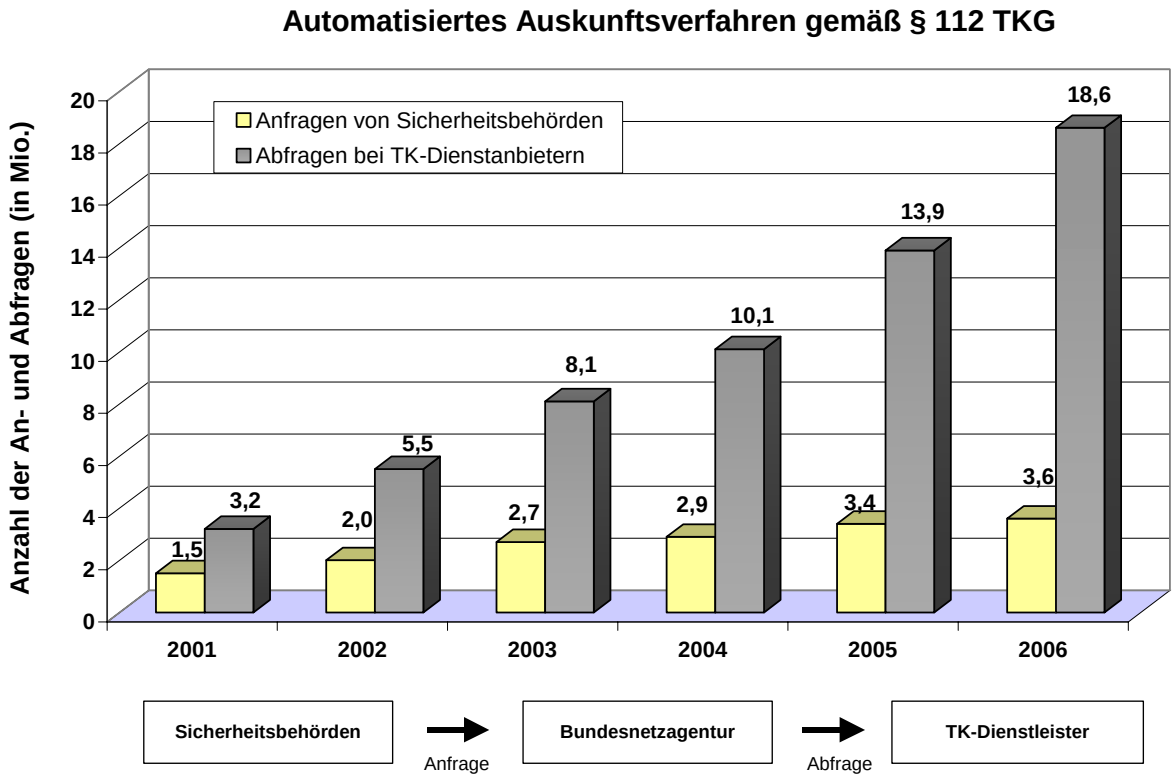
Bestellung des betrieblichen Datenschutzbeauftragten	Unternehmen
Zusendung von Werbung nach Teilnahme an Preisausschreiben	Bürgerin
Videoüberwachung an Zahlstellen einer Behörde	Bürger und Beschäftigte
Veröffentlichung von Bilddaten über Wohngebäude im Internet	Haus- bzw. Wohnungseigentümer
Erhebung von Verbrauchsdaten bei den Stadtwerken zur Erstellung eines Energieausweises durch Vermieter	Hauseigentümer und Mieter
Bestellung externer behördlicher Datenschutzbeauftragter	Unternehmen
Erhebung von Daten für den Mikrozensus	Bürgerin
Weitergabe von statistischen Einzelangaben an Wohnungsgesellschaften	Wohnungsinhaber
Aushang über die Teilnahme von Betriebsratsmitgliedern an Fortbildungsveranstalten durch den Geschäftsführer	Betriebsratsmitglieder bzw. Beschäftigte
Wegfall des Personenbezugs bei der Übermittlung von Daten zur Erstellung eines Energieausweises	Wohnungsinhaber
Weitergabe von Mitgliederdaten innerhalb einer Partei	Parteimitarbeiter
Wirksamkeit einer Schweigepflichtentbindungsklausel gegenüber einer Krankenasse	Versicherungsnehmer
Übertragung von Funktionen auf ein Call Center	Kunden, Beschäftigte
Auskunft über personenbezogene Daten an einen Bevollmächtigten	Behörde
Selbstauskunft bei einer Auskunftei	Bürger
Verkauf einer umgetauschten bespielten Festplatte als neu	Bürgerin
Registermeldung nach § 4 d BDSG	Unternehmen
Auskunftspflicht beim Mikrozensus	Bürger
Aushang eines Arbeitsgerichtsurteils mit personenbezogenen Daten im Betrieb	Beschäftigter
Übermittlung personenbezogener Verbrauchsdaten an Hauseigentümer zur Erstellung eines Energieausweises durch Energieversorgungsunternehmen	Mieter
Erforderlichkeit der Einwilligung bei Cookies und Personenbezug bei der IP-Adresse	Beschäftigte, Nutzer
Veröffentlichung von vollständigen Namen und Fotos auf der Homepage des Arbeitgebers	Beschäftigte
Einsicht in das Profiling	ALG II-Empfänger
Vorlage und Anfertigung von Kopien der Kontoauszüge	ALG II-Empfänger
Übermittlung von Unternehmensdaten an nicht öffentliche Stellen durch die Handelskammer	
Speicherung von IP-Adresse zur Nutzung von Abmahnungen	Betroffener
Übermittlung von Betroffenendaten an Auskunftei in Bremen	Unternehmen
Datenschutz bei Bewährungshilfe	Betroffener
Versendung eines Kaufvertrages an falsche E-Mail-Adresse durch Notariat	Käuferin
Verschaffung von Daten zum Zwecke der Abmahnung durch Inkassobüro	Betroffener
Verweigerung einer Auskunft nach § 34 BDSG mit Hinweis auf den Datenschutz durch ein Kreditinstitut	Antragsteller für einen Kredit
Zugang zum Intranet	bremische Gesellschaft
Weitergabe von Mitarbeiterdaten an das Integrationsamt	Beschäftigte

Speicherung der IP-Adresse durch Rechteinhaber und Abmahnung	Betroffene (4 Personen)
Veröffentlichung von Kontrakten mit Forschungseinrichtungen im Internet	Beschäftigte, Inhaber von Forschungseinrichtungen
Beleidigende Äußerungen in Internetforum	Betroffene
Vorlesen der Namen aus Krankmeldungen gegenüber anderen Beschäftigten	Beschäftigte
Einzelgebührennachweis über Telefongespräche im Betrieb	Beschäftigte
Auskunft aus dem polizeilichen Informationssystem	Bürger
Einsicht in Strafakten ohne Vollmacht durch einen Rechtsanwalt	Beschuldigter
Geltung des BremDSG für die Personaldatenverarbeitung in Kliniken	Beschäftigte
Vorlage einer Vollmacht zur Einsichtnahme in die Personalakte durch den behördlichen Beauftragten für Datenschutz	Beschäftigter
Veröffentlichung von Schülerfotos im Internet	SchülerInnen
Verarbeitung von Heizungsverbrauchsdaten zur Erstellung eines Energieausweises	Mieter
Formularschreiben zu Recht auf Auskunft bei öffentlichen und nicht öffentlichen Stellen	Betroffene
Datenspeicherung durch Auskunftei in Bremen	Betroffener
Nutzung von Daten für Werbezwecke	Betroffener
Vorlage des Einkommenssteuerbescheides zur Berechnung des Krankenkassenbeitrages	Versicherter

24.3 Anstieg der Telefonüberwachung



Die aktuellen Zahlen der tatsächlich in 2007 durchgeführten Maßnahmen der Telefonüberwachung liegen noch nicht vor. Meine im letzten Jahresbericht abgegebene Schätzung von 40.000 (vgl. 29. JB, Ziff. 22.3) wurde noch 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. Im abgebildeten Diagramm ist die Entwicklung beim automatisierten Auskunftsverfahren gemäß § 112 TKG im Zeitraum 2001 bis 2006 dargestellt.

24.4 Indikatoren der Informationsgesellschaft[1]

Land	ITK[2]-Umsatz	PC	Internet-Nutzer[3]	Mobil-Telefone[4]	DSL-Anschlüsse[5]	WLAN-Hotspots[6]
	in Prozent des BIP	je 100 Einwohner			je 100 Haushalte	je 100.000 Einwohner
D	6,2	43	58	95	26	10
DK	6,5	64	77	97	33	17
E	5,9	22	41	98	25	3
F	6,0	39	50	77	35	6
FIN	7,0	47	69	102	40	7
I	5,3	25	56	118	28	3
S	8,6	63	74	110	26	7
UK	8,0	46	66	110	30	21
Osteuropa[7]	.	.	13	62	.	.
CH	7,7	58	55	88	32	17
N	5,3	64	71	107	37	8
J	7,7	50	53	74	31	3
USA	6,6	84	68	71	16	12

[1] Stand 2005; [2] Informationstechnik und Telekommunikation; [3] Personen mit Zugang zum Internet, ohne drahtlose Internet- und alleinige Intranetnutzung; [4] Subskriptionen (inkl. Prepaid-Karten) in analogen und digitalen Mobilfunknetzen; [5] breitbandige Kommunikation (Digital Subscriber Line) einschl. Unternehmensanschlüsse; [6] Wireless Local Area Network: örtlich begrenzte Funknetze, die einen drahtlosen, schnellen Internetzugang ermöglichen; [7] EU-Beitrittsländer und andere osteuropäische Staaten

Quelle: BITKOM Institut der deutschen Wirtschaft Köln

24.5 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: 0471 596 - 2010 / 0421 361 - 2010

Telefax: 0421 496-18495

E-Mail: office@datenschutz.bremen.de

angefordert werden:

26. Jahresbericht 2003, Bürgerschafts-Drs. 16/189 (Restexemplare)

27. Jahresbericht 2004, Bürgerschafts-Drs. 16/578 (Restexemplare)

28. Jahresbericht 2005, Bürgerschafts-Drs. 16/980 (Restexemplare)

29. Jahresbericht 2006, Bürgerschafts-Drs. 16/1362 (Restexemplare)

Broschüre „Orientierungshilfe – Datenschutz bei Dokumentenmanagementsystemen"

Faltblatt „Das Informationsfreiheitsgesetz des Bundes“

Faltblatt „Datenschutz bei der Polizei“

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 „Datenschutz bei der Internet-Telefonie“

Faltblatt „Keine Spione auf der Festplatte“

Faltblatt „Verräterische Spuren auf Festplatten“

Faltblatt „Videoüberwachung durch private Stellen“

Faltblatt „Surfen am Arbeitsplatz – Datenschutz-Wegweiser“

BfDI – Info 1 Bundesdatenschutzgesetz - Text und Erläuterungen -

BfD – Info 2 Informationsfreiheitsgesetz - Text und Erläuterungen -

BfD – Info 4 Die Datenschutzbeauftragten in Behörde und Betrieb

Die Broschüren BfDI – Info 1, 2 und 4 können beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit auf dessen Homepage (www.bfdi.bund.de) eingesehen und heruntergeladen werden.

24.6 Fremdwort- und Abkürzungsverzeichnis

In der Regel werden in den Artikeln bereits die Abkürzungen erklärt. Diese werden daher nicht noch einmal in diesem Abkürzungsverzeichnis aufgenommen. Mit aufgenommen werden Erklärungen für Fremdworte (z. B. AOL...).

Abkürzung	**Erklärung**
ALG	Arbeitslosengeld
AOK	Allgemeine Ortskrankenkasse
AOL	Internet-Unternehmen
ARGE	Arbeitsgemeinschaft nach § 44 b SGB II
Art. 29-Gruppe	Unabhängiges Beratungsgremium der Europäischen Union in Datenschutzfragen
BaföG	Bundesausbildungsförderungsgesetz
BAgIS	Bremer Arbeitsgemeinschaft für Integration und Soziales
BDSG	Bundesdatenschutzgesetz
Biometrie	Mess- und Auswerteverfahren an Lebewesen; eingesetzt zur Identifizierung von Individuen
BKA	Bundeskriminalamt
BN	Bremer Nachrichten (Tageszeitung)
BONITAET	IT-Verfahren zur IT-unterstützten Auswertung entgegengenommener Verpflichtungserklärungen
BREKOM	Bremer Kommunikationstechnik GmbH
BremIFG	Bremer Informationsfreiheitsgesetz
BVerfGE	Entscheidungen des Bundesverfassungsgerichtes
BVN	Bremer Verwaltungsnetz
BZR	Bundeszentralregister
CD	Compact Disc; optisches Speichermedium
CDU	Christlich Demokratische Union Deutschlands (Partei)
CeBIT	Computermesse
Dataport	Dienstleister für Informations- und Kommunikationstechnik der öffentlichen Verwaltung in Schleswig-Holstein, Hamburg und Bremen sowie (teilweise) in Mecklenburg-Vorpommern
DoubleClick	Online-Werbevermarkter
DSB	Datenschutzbeauftragter
DV	Datenverarbeitung
DVD	Digital Versatile Disc; digitales, optisches Speichermedium ähnlicher der CD, aber mit höherer Speicherkapazität
DVU	Deutsche Volksunion (Partei)
eBay	Internetauktionshaus
EDV	Elektronische Datenverarbeitung
EDV-Support	Unterstützung (Dienstleistung) im EDV-Bereich
EG	Europäische Gemeinschaft
E-Government	Elektronische Verwaltungsanwendungen, meistens Internet-basiert

ELSTER	Elektronische Steuererklärung
E-Mail	Elektronische Post
Europol	Europäische Polizeibehörde
Google	Internet-Suchmaschine
Google-Earth	Virtueller Globus bestehend aus Satellitenbildern
GPS	Global Postioning System; satellitengestütztes System zur weltweiten Positionsbestimmung
ICD-Schlüssel	International Statistical Classification of Diseases and Related Health Problems; Internationale Klassifikation der Krankheiten und verwandter Gesundheitsprobleme
IP-Adressen	Internet-Protocol-Adresse; dient zur eindeutigen Adressierung von Computern in Netzwerken, u. a. dem Internet
IT	Informationstechnologie
KpS	Kriminalpolizeiliche Sammlung
LfV	Landesamt für Verfassungsschutz
Log-Datei	Protokolldatei in Computersystemen
Mammographie-Screening	Reihenuntersuchung der Brust bei Frauen zwischen 50 und 69 Jahren
Mikrozensus	repräsentative statistische Erhebung
NSA	National Security Agency; US-amerikanischer Nachrichtendienst, zuständig für die weltweite Überwachung und Entschlüsselung elektronischer Kommunikation
OSCI	Online Services Computer Interface; sichere und vertrauliche Übertragung digital signierter Dokumente über das Internet
Passwort	Kennwort, Codewort
PC	Personalcomputer
Petent	Bürger der eine Beschwerde einlegt
PIN	Persönliche Identifikationsnummer
PNR	Passenger Name Record; Passagierregister
RFID	Funkchip
Rollout	Einführung, Markteinführung
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
Scoring	Nutzung analytisch statistischer Verfahren für Risikoabschätzungen
Second Life	Online-Spiel im Internet
Security-Gateway	Vermittlungsgerät zwischen Rechnernetzen mit Sicherheitsfunktionen
Service Desk	zentrale Stelle für Nutzerunterstützung im IT-Bereich
SGB	Sozialgesetzbuch
Smartcards	Spezielle Plastikkarte mit eingebautem Chip, enthält in der Regel Speicherplatz und einen Mikroprozessor
StaLa	Statistisches Landesamt
StPO	Strafprozessordnung
SWIFT	Society for Worldwide Interbank Financial Telecommunication; internationale Genossenschaft der Geldinstitute; betreibt ein Telekommunikationsnetz für weltweite Finanztransaktionen
Ticketsystem	System zur Verwaltung von Serviceaufträgen
TÜPFO	Schreibsoftware, eingesetzt in der Telekommunikationsüberwachung
VwVfG	Verwaltungsverfahrensgesetz

WK	Weser Kurier (Tageszeitung)
World of Warcraft	Internet-Onlinespiel
ZFER	Zentrales Fahrerlaubnisregister
ZGF	Bremische Zentralstelle für die Verwirklichung der Gleichberechtigung der Frau
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister

24.7 Index