BREMISCHE BÜRGERSCHAFT **Drucksache 17 /706**
Landtag 27. 02. 09
17. Wahlperiode

31. Jahresbericht des Landesbeauftragten für Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats über das Ergebnis der Tätigkeit im Jahre 2008 den 31. Jahresbericht zum 31. März 2009 (§ 33 Abs. 1 Bremisches Datenschutzgesetz – BremDSG). Redaktionsschluss für die Beiträge war der 1. Dezember 2008.

Sven Holst
Landesbeauftragter für Datenschutz und Informationsfreiheit

Inhaltsverzeichnis

1. Vorwort

1.1 Blick auf das Jahr 2008

Der Blick auf das Jahr 2008 fällt nachdenklich aus. Ja, der Datenschutz konnte viele Erfolge verzeichnen: Der Bericht gibt eine ganze Reihe davon wieder. Datenschutzjubiläen, wie 25 Jahre Volkszählungsurteil, gelungene Veranstaltungen mit Schülerinnen und Schülern in Bremerhaven am europäischen Datenschutztag, das in Bremen abgeschlossene „Profiler-Projekt" zu den neuen Formen und Gefahren der Identitätsausbeute mit hoher Resonanz in der Bremer Bevölkerung, sind nur einige. Aber auch viele zähe, sich jetzt schon über Jahre hinziehende Verhandlungen mit Spitzenverbänden der Wirtschaft, so dass häufig die Verhandlungsergebnisse schon bald wieder von der technischen Entwicklung überrollt werden, ein Bundesgesetzgeber, der die Ränder der Verfassung immer wieder austestet und vom Bundesverfassungsgericht wiederholt zurückbeordert werden musste und, nicht zu vergessen, die Datenschutzskandale, beginnend im Frühjahr mit dem Bekannt werden der Arbeitnehmerüberwachung bei Lidl, gefolgt von illegaler Überwachung mit Verbindungsdaten bei der Telekom.

Ja, die Telekom ist wohl mit Abstand der größte Verlierer im Jahr der Datenpannen und des Datenklaus, denn der Telekom kamen wohl die meisten Daten abhanden. Auch wenn diese Daten bei verschiedenen Callcentern, Adresshändlern oder im Internet auftauchten und die Staatsanwaltschaft die Daten an diesen Orten beschlagnahmte, muss doch davon ausgegangen werden, dass der größte Teil der Daten verloren bleibt, denn es ist wahrscheinlich, dass weitere Kopien existieren, die unter der Hand vermarktet wurden. Das Kind „Vertrauen" ist in den Brunnen gefallen, auch wenn das Management sich jetzt intensiv bemüht, den Datenschutz im Unternehmen auf Vordermann zu bringen.

Auch beim Datenskandal eines Berliner Bankhauses reibt man sich ungläubig die Augen: Jeder 5-Euro-Schein wird schwer bewacht und sicher verpackt in gepanzerten Fahrzeugen transportiert. Große Mengen sensibler Kundendaten hingegen gibt man zum Versand bei der Post auf.

Erschreckend ist, dass gerade Unternehmen mit besonderen Geheimhaltungsregeln, nämlich dem Telekommunikations- und dem Bankgeheimnis, die älter als die allgemeinen Datenschutzvorschriften sind, durch besonders laxen Umgang mit geschützten Daten auffielen.

Nicht umsonst schaffte das Wort „Datenklau" es immerhin auf Platz 3 der Top Ten der Worte des Jahres. Bei den Datenschutzbeauftragten wie bei den -aufsichtsbehörden sorgten die mit dem Wort verbundenen Datenskandale im zweiten Halbjahr für Hochkonjunktur. Sicherlich, die Bevölkerung ist von den Datenschutzthemen aufgerüttelt, aber wir, die wir wissen, dass es nur die Spitze des Eisbergs ist, die sichtbar wurde, allein wenn wir in die Tiefen des Internets schauen, wissen nicht, ob wir uns über das Erreichte freuen können, denn die permanente und rapide informationstechnologische Entwicklung macht einen Datenschutz auf Augenhöhe der technischen Entwicklung fast ausgeschlossen, jedenfalls so lange, wie sich nicht die Systementwickler und Datenverarbeiter selbst mit an die Spitze der Datenschutzbewegung setzen.

Auch wenn die Datenschutzskandale zu beklagen sind, wenn viele Betroffene dadurch auch materiellen Schaden genommen haben, hat doch all das dazu beigetragen, dass die Unterstützung des Datenschutzes seitens der Politik wie der Bürgerinnen und Bürger stark zugenommen hat.

Wesentlich anders als bei Teilen der Wirtschaft und im Bund sieht die Situation zurzeit im öffentlichen Bereich in Bremen und Bremerhaven aus. Zwar wird hier und da immer wieder vergessen, den Datenschutz schon in der Projektphase zu implementieren, in einzelnen Bereichen muss auch noch zäh für ein Datenschutzbewusstsein gerungen werden, aber in vielen Bereichen auch der Führungsebenen finden nicht mehr wie früher lange Diskussionen über das „Ob" statt, sondern es wird immer häufiger gefragt, was für einen guten Datenschutz zu tun ist, und dann wird das auch zügig umgesetzt. Auch im Bereich der inneren Sicherheit werden in letzter Zeit nicht wie in anderen Bundesländern dauernd die gesetzlichen Befugnisse für Eingriffe in das Recht auf informationelle Selbstbestimmung erweitert, sondern, wie in diesem Jahr geschehen, es wurde die verfassungswidrige Regelung zum Kfz-Kennzeichenscan im Bremischen Polizeigesetz umgehend ersatzlos gestrichen.

Nicht zu unterschätzen sind die Pionierleistungen, die Bremen, auch in Abstimmung mit meinem Haus, bundesweit auf dem Gebiet des E-Governments auf den Weg gebracht hat und dessen Früchte einer sicheren Kommunikation seit geraumer Zeit geerntet werden können. Es ist nicht zu verkennen, ein Teil der Probleme mit dem Datenschutz rührt daher, dass im Land Bremen gespart werden muss und daher auch die informationstechnischen Projekte unter engen personellen und sachlichen Bedingungen vorangetrieben werden müssen. Oft geht es darum, dass ein System bis zu einem bestimmten Termin funktionstüchtig bereitstehen muss. Und in dieser Not wird dann auch am Datenschutz gespart. Die Aufgabe des Landesdatenschutzbeauftragten ist es aber nicht, sich damit abzufinden, und deshalb lasse ich in solchen Fällen, auch wenn es der Verwaltung häufig „auf die Nerven geht", nicht locker, bis der Datenschutz nachgebessert wurde. So wurden z. B. in den letzen Jahren schrittweise für einzelne Module im Stadtamt Bremen Datenschutzkonzepte erstellt, nun zeichnet sich in diesem Jahr ab, dass auch das fehlende Bindeglied, das Rahmendatenschutzkonzept, seiner Vollendung zustrebt. Ein Thema, mit dem sich der parlamentarische Ausschuss für den Datenschutz leider immer wieder beschäftigen musste, strebt damit seiner Lösung zu.

Mit dem Referat 36 der Senatorin für Finanzen, das als zentrale Schnittstelle die IT-Infrastruktur des Landes Bremen maßgeblich gestaltet, hat im Berichtsjahr eine enge Kommunikation mit meiner Dienststelle stattgefunden. Komplexe Veränderungen der Infrastruktur, wie die Auslagerung bremischer Verfahren zum Dienstleister Dataport, die Zentralisierung der E-Mail-Kommunikation und die Einführung eines neuen Verzeichnisdienstes (Active Directory), erforderten neben der Klärung von Grundsatzfragen und der Festlegung datenschutzrechtlicher Anforderungen in Konzepten auch einen ständigen Austausch während des Einführungsprozesses. In dem Spannungsfeld zwischen Wirtschaftlichkeit, Effizienz, technologischer Qualität und Datenschutz ist es trotz massiven Zeitdrucks gelungen, einvernehmlich konstruktive Lösungen zu finden.

1.2 Kurzer Rückblick auf die Projekte der letzen acht Jahre

In den vergangenen Jahren habe ich neben den Beratungs- und Kontrollaufgaben immer parallel weitere Ziele zur Effektivierung und Leistungsverbesserung meiner Dienstelle und des Datenschutzes verfolgt.

— Begonnen habe ich mit der Verstärkung der Internetpräsenz durch den Auf- und Ausbau der Homepage des Landesbeauftragten für Datenschutz. Durch diese Maßnahme habe ich eine spürbare Entlastung bei Standardanfragen erreicht.

— Maßgeblich habe ich mich an der konzeptionellen Entwicklung der bis Mitte 2008 landeseigenen Gesellschaft „datenschutz nord" beteiligt.

— Dann kam das Jubiläumsjahr 2003: Mit der Herausgabe der CD-ROM „25 Jahre Datenschutz im Land Bremen" habe ich zwei Ziele verbunden. Zum einen den Rückblick auf die Entwicklung im legislativen Bereich im Land Bremen – ich erinnere nur an die bundesweit richtungsweisenden Datenschutzregelungen im Bremischen Polizei- wie auch im Bremischen Verfassungsschutzgesetz –, einem Rückblick auf die Arbeit des parlamentarischen Datenschutzausschusses (alle Vorsitzenden waren bereit, das jeweils in einer Legislaturperiode Erreichte darzustellen), einem Rückblick auf die Arbeit der Senatskommissare für den Datenschutz und einem Rückblick auf die vor mir amtierenden Datenschutzbeauftragten, die mit beachteten Beiträgen auf die Situation im Datenschutz eingingen oder aber einen real-futuristischen Ausblick auf die Zukunft des Datenschutzes warfen. Zum anderen enthielt die CD-ROM erstmalig in elektronischer Form die bis dahin erschienenen Jahresberichte. Damit war es einfach geworden, auf die doch häufigen Anfragen auf Übersendung von Datenschutzberichten zu reagieren, nicht nur, dass die Erstellung der CD mit allen Jahresberichten günstiger war als der Druck eines Berichts auf Papier, auch das Porto für den Versand war deutlich geringer. Im gleichen Jahr habe ich dann die elektronisch erfassten Berichte auch auf meine Homepage übernommen.

— Ein seit Inkrafttreten der Vorschriften über die behördlichen Datenschutzbeauftragten 2003 verfolgtes Projekt ist die Durchführung von Workshops mit den behördlichen Datenschutzbeauftragten, um so deren Eigenständigkeit zu stärken. Die Workshops werden zwei- bis dreimal im Jahr durchgeführt, enthalten einen Schulungsteil, den meine Dienststelle durchführt, und sind verbunden

mit einem daran anschließenden Erfahrungsaustausch. Die im Rahmen der Unterrichtung über die Aufgaben gehaltenen Vorträge werden – ergänzt um die Ergebnisse der Diskussion – auf meiner Homepage veröffentlicht, um so behördlichen Datenschutzbeauftragten, die nicht teilnehmen konnten oder die erst neu hinzugekommen sind, die Möglichkeit zu geben, sich auf diese Weise zu informieren. So stehen unter der Rubrik „Hilfestellungen" bereits eine ganze Reihe von im Hause erarbeiteten Orientierungshilfen und Merkblättern für die Aufgaben der behördlichen Datenschutzbeauftragten zur Verfügung.

— Das nächste von mir in den Jahren 2002/2003 angegangene Projekt mit dem Titel „Selbstverteidigung im Internet" zielte darauf ab, den Bürger bei der Wahrnehmung seines informationellen Selbstbestimmungsrechts im Internet zu unterstützen. Es reicht nämlich nicht aus, wenn man seine Rechte kennt, im Internet muss man sie auch durchsetzen können. Datenschutz sollte bei einem in der Familie gemeinsam genutzten PC beginnen, u. a. mit der Vermeidung von Datenverlusten durch Virenattacken weitergehen und sich fortsetzen bei der Abwehr von Hackerangriffen und von Ausforschungsprogrammen, die sich im Rechner einnisten. Es waren daher Verhaltensregeln und insbesondere technische Maßnahmen, wie zum Beispiel die richtige Einstellung des Internetbrowsers und der Firewall und anderer Sicherheitssoftware Themen, die bei dieser Aktion im Vordergrund standen. Wegen der sich laufend ändernden Technik und der immer wieder neu hinzukommenden Gefahren durch Attacken aus dem Internet auf die Rechner wird dieser Bereich meiner Homepage regelmäßig angepasst und ergänzt.

— Im folgenden Jahr wurde das Projekt um weitere Facetten rund um den heimischen PC ergänzt. Mit dem Projekt „Family-PC" wurden die, wenn auch begrenzten Möglichkeiten zur Erreichung von Datenschutz etwa durch die Einrichtung verschiedener Benutzergruppen für einzelne Familienmitglieder oder der Einstellung des Browsers dargestellt, damit nicht jeder weitere Nutzer des PC schauen kann, welche Internetadressen der Vorgänger in den letzten Wochen oder gar Monaten angewählt hat.

— Dann folgte das Projekt „datenschutz4school", mit dem ich Schülerinnen und Schüler auf der Ebene ihres alltäglichen Tuns abhole und sie für Fragen des Datenschutzes interessiere. Die Darstellungen sind animiert, die einzelnen Kapitel werden durch die Bremer Stadtmusikanten begleitet. Am Ende können innerhalb der Anwendung durch das richtige Beantworten von Datenschutzfragen gewonnene Punkte in einer Slotmaschine verspielt werden. Die Besten können sich in einer Top Ten-Liste mit Namen, Schule und Punktzahl eintragen. Im Moment liegt das Schulzentrum Grenzstraße mit 6 Einträgen vorn. Da „datenschutz4school" gerade auch im Unterricht zum Einsatz kommen soll, ist auch eine Lehrhilfe hinterlegt, mit der den Lehrkräften die Methodik und die Lernziele erläutert werden. Zurzeit zählen wir 23 000 Zugriffe, die tatsächlichen Zugriffszahlen dürften deutlich höher liegen, weil oft ganze Klassen über Proxy-Server die Anwendung nutzen.

— Dann musste das Projekt „Erste Homepage für die Bremer Informationsfreiheit" angegangen werden. Im Frühjahr 2006 wurde das Bremer Informationsfreiheitsgesetz verabschiedet. Es gelang parallel zum Inkrafttreten, die Internetseite „www.informationsfreiheit.de" zu starten und so den in Bremen und Bremerhaven lebenden Bürgerinnen und Bürgern eine erste Anlaufstelle für alle Fragen rund um die Informationsfreiheit zu geben. Der Senat hat erst wesentlich später dazu etwas auf seiner Homepage angeboten. Ich nenne dieses Projekt an dieser Stelle, weil die finanziellen, insbesondere aber die personellen Ressourcen aus dem Bereich des Datenschutzes geschöpft werden mussten.

— In 2008 konnte endlich die Doppelbroschüre Datenschutz/Informationsfreiheit mit den für Bremen geltenden einschlägigen Gesetzesregelungen und versehen mit Vorwort und Erläuterungen zu beiden Bereichen angeboten werden. Der Bedarf war, wie sich zeigte, groß, die ersten 700 Exemplare waren schnell vergriffen, es mussten noch in 2008 1000 Broschüren nachgedruckt werden. Durch Sponsoring konnten die Kosten pro Heft minimiert werden.

— Schließlich habe ich im Berichtsjahr das Projekt „Profile" entwickelt, um die Bürgerinnen und Bürger in ihren verschiedenen Rollen als Konsumenten, Arbeitnehmer, Reisende oder Internetsurfer auf die mit der aktuellen technischen Entwicklung einhergehenden neuen Gefahren für ihr Recht auf informationelle

Selbstbestimmung aufmerksam zu machen und als „Erste Hilfe“ benannte Abwehrstrategien aufzuzeigen. Näheres finden Sie im Beitrag unter Ziff. 1.3 dieses Berichts und natürlich auf meiner Datenschutz-Homepage. Die einzelnen Beitragsteile wurden jeweils auf den Verbraucherseiten einer Bremer Tageszeitung vorgestellt.

Natürlich können nicht alle Internetprojekte gleichmäßig auf dem neuesten Stand gehalten werden, aber immerhin ist es gelungen, meine Homepage in Abständen von ca. drei Jahren zu aktualisieren. Das ist angesichts der rasch fortschreitenden technischen Entwicklung das Äußerste, was hinnehmbar ist.

1.3 Mit Datenschutz gegen heimliche Profilbildung

In einer zunehmend technisch geprägten Welt lassen sich die allgegenwärtigen IT-Systeme in ihrer Komplexität durch den Einzelnen immer schwerer beherrschen. Alle Bürgerinnen und Bürger, die moderne Techniken anwenden – bei Kommunikation, Mobilität, Einkauf oder bloßer Information –, geben gewollt oder ungewollt Daten über sich preis und hinterlassen jede Menge digitaler Spuren. Ob Internetsuchmaschine oder „Blog“, Bahncard oder Rabattkarte, ob Fernsehen via DSL, Handy oder Navigationsgerät: Menschen erzeugen Daten, die – systematisch gesammelt und zu sogenannten Profilen gebündelt – sie dann ein Leben lang verfolgen können. Aber die wenigsten Menschen sind sich im Klaren darüber, dass sie damit „gläsern“ und zum Opfer von Datenjägern werden können. Die Profilbildung (Profiling) geschieht nämlich meistens ohne Wissen der Betroffenen.

Im vergangenen Halbjahr habe ich daher in Teamarbeit das Projekt „Profile“ entwickelt und in den sieben Wochen vor Weihnachten auf der Datenschutz-Homepage www.datenschutz.bremen.de sukzessive freigeschaltet. Das Projekt hat den Anspruch, den Bürgerinnen und Bürgern bewusst zu machen, dass es solche „Profiler“ gibt – und ihnen zu zeigen, wie sie sich dagegen soweit wie möglich schützen können. Die jüngsten Fälle von Datenmissbrauch machen deutlich: Es ist für die Bürgerinnen und Bürger völlig egal, ob ihre Daten legal erfasst oder illegal abgesaugt werden. Denn die „Profile“, die man daraus erstellen kann, und die darauf aufbauende Datennutzung sind längst zu einer lukrativen Wirtschaftsbranche geworden. Nur wenn die Betroffenen lernen, die Erzeugung solcher Daten zu vermeiden oder aber ihre Spuren zu löschen, haben sie eine Chance, Herr ihrer Daten zu bleiben.

In dem Projekt werden daher, mit provokanten Überschriften versehen, nüchterne technische Sachverhalte ansprechend dargestellt und dabei nicht nur die nachweisbaren, sondern auch mögliche, mit der Entwicklung verbundene künftige Risiken angesprochen. Überschriften wie „Verkaufen Sie sich nicht, wenn Sie einkaufen“, „Alles unter Kontrolle – Sie auch“ oder „Gläserne Bürger machen Demokratie zerbrechlich“ verdeutlichen dies. Zu jeder der sieben Einheiten wurde eine „Erste Hilfe“ für die Bürgerinnen und Bürger veröffentlicht, in der sowohl besonders risikoreiches Verhalten als auch Möglichkeiten der Gefahrenabwehr dargestellt werden.

In Kooperation mit der Redaktion der Bremer Tageszeitungen („Weser-Kurier“ und „Bremer Nachrichten“) erschien – parallel zu den Veröffentlichungen auf meiner Homepage – eine siebenteilige Artikelserie der Redaktion auf der Verbraucherseite unter dem Logo „VERRATEN UND VERKAUFT“. Mit dieser Serie ist es gelungen, mehr oder weniger umfassend und bundesweit erstmalig die neuen technischen Entwicklungen, mit denen die Bürgerinnen und Bürger konfrontiert sind, zusammenfassend darzustellen und die damit verbundenen Datenschutzrisiken aufzuzeigen.

Die mit der Serie gestiegenen Zugriffszahlen auf meine Homepage verdeutlichen das Interesse der Bevölkerung. Ich hoffe, dass ich die Bürgerinnen und Bürger ein bisschen wachrütteln konnte. Vielleicht haben sie so erst die notwendigen Sicherheitseinstellungen an ihrem neuen PC vorgenommen, der auf dem Gabentisch lag, bevor sie sich mit den Worten „Ich bin schon drin“ ins World Wide Web begeben haben.

Themen der Serie (in Klammern das Erscheinungsdatum) sind:

Google und andere Suchmaschinen	(06.11.2008)
ID-Management	(13.11.2008)
Location Based Services	(20.11.2008)

RFID	(27.11.2008)
Konvergenz von Techniken & Netzen	(04.12.2008)
Ubiquitäres Computing	(11.12.2008)
Soziale Netzwerke – Web 2.0	(18.12.2008)

1.4 Kein Datenschutz ohne Datensicherheit

Ein ausreichender Datenschutz ohne Datensicherheit wäre nicht zu denken. Das Ziel ist immer das gleiche: Sicherheit für Unternehmensdaten, Sicherheit für personenbezogene Daten, Sicherheit für Unternehmensinfrastrukturen, Sicherheit für Verwaltungsinfrastrukturen, Sicherheit für nationale Infrastrukturen. Auch die Methoden, um die Ziele zu erreichen, sind weitgehend deckungsgleich. Soweit der einfache Teil der Betrachtung, denn die Anzahl der möglichen Anwendungen und deren Einsatzkontexte sind unbegrenzt. Extrem schwierig wird es, wenn es darum geht festzulegen, welche konkreten Methoden angemessen sind, um das Ziel „Sicherheit" zu erreichen. Zumal ständig und permanent neue Sicherheitsgefahren mit immer noch zunehmender Geschwindigkeit auftauchen.

Da den Überblick zu behalten, ist selbst für Spezialisten nicht einfach. Da gibt es Innentäter und Außentäter, zeit- und sicherheitskritische Anwendungen, über mehrere Standorte verteilte Anwendungen, die auch noch vollständig mobil zu nutzen sind, und irgendwie hängt alles auch immer mit dem Internet zusammen. Hier ein paar Zahlen, die ich ähnlich auf dem 16. BremSec-Forum in Bremen vorgetragen habe.

Umfragen zeigen:

— Die gegenüber deutschen Unternehmen aufgedeckten Straftaten im IT-Bereich summieren sich auf einen Schaden von 6 Milliarden Euro pro Jahr,

— fast 50 % aller deutschen Unternehmen haben in den vergangenen beiden Jahren Schäden durch Wirtschaftskriminalität erlitten,

— rund 50 % aller Täter stammen aus dem eigenen Unternehmen,

— früher handelte es sich mehr um „Fun-Täter", heute wird der wirtschaftliche Vorteil gesucht.

Die Gefahrenlage:

— Die Anzahl von Schadprogrammen sowie die Summe der Schwachstellen in IT-Produkten (Hardware, Software) verdoppeln sich mindestens jährlich,

— fast jede zehnte E-Mail ist mit Malware (Viren, Würmer) verseucht,

— mehr als 90 % aller E-Mails weltweit sind Spams.

— der Trend geht zu unauffälligen Spionageprogrammen (Trojaner, Bot-Netze), die für kriminelle Zwecke eingesetzt werden,

— mobile Endgeräte verschieben Unternehmensgrenzen und stellen ein qualitativ neues Risiko dar,

— die generellen Möglichkeiten von Angriffen auf zentrale IT-Strukturen steigen durch zunehmende Nutzung von Standardsystemen und -software in kritischen Bereichen.

Doch trotz der gestiegenen Risiken für die IT verzichten gerade mittelständische Unternehmen auf geeignete Schutzmaßnahmen! (Ergebnisse einer Umfrage von PWC unter 8200 IT-Verantwortlichen aus 63 Ländern)

— Die sicherheitsbezogenen IT-Vorfälle stiegen um 22,4 %,

— ca. 24 % erlitten dadurch finanziellen Schaden (Vorjahr: 7 %),

— Befragte aus Deutschland bezifferten den jeweils erlittenen Schaden im Einzelfall auf bis zu 500 000 € und bestätigten Ausfallzeiten von bis zu 8 Stunden.

Aber

— nur etwa 13 % der Investitionen fließen in den IT-Bereich (Vorjahr: 15 %),

— nur jedes 3. Unternehmen hat tatsächlich einen IT-Notfallplan,

— weltweit will jedes 2. Unternehmen mehr in IT-Sicherheit investieren, in Deutschland nur jedes 3. Unternehmen.

(Diese Darstellung beruht auf Auswertungen von Publikationen der NIFISeV und PriceWaterhouseCoopers/Martin-Luther-Universität, Wirtschaftskriminalität 2007.)

Für Unternehmen und Verwaltungen bleibt oft nichts anderes übrig, als auf externe Dienstleister zurückzugreifen, um etwaige Risiken zu bewerten und sich dagegen abzusichern. Ansonsten stehen viele IT-Verantwortliche oft allein auf weiter Flur, obwohl die grundsätzlichen Fragestellungen überall die gleichen sind. Da macht es Sinn, sich, wie auf dem BremSec-Forum geschehen, zu treffen und zu hören, aber auch zu berichten, welche Probleme man wie bearbeiten kann. Das sichert einen leichten Informationsfluss von Know-how-Trägern und dient insgesamt der Sache: „IT-Sicherheit und Datenschutz". Ich unterstütze daher solche Initiativen nach Kräften, denn in solchen Netzwerken lassen sich die wachsenden Probleme am besten kommunizieren und Lösungen diskutieren.

1.5 Datenschutz steht heute vor ganz neuen Herausforderungen

Früher ging es darum, die Betreiber von Großrechenanlagen/Rechenzentren und darauf folgend um Arbeitsplatzcomputer für einen verantwortungsbewussten Umgang mit der Technik und den dort gespeicherten Daten zu gewinnen. Heute befinden sich mannigfaltige Geräte, die personenbezogene Daten erzeugen und verarbeiten, in vielen Händen: Neben den Unternehmen und staatlichen Stellen jetzt auch in privaten Haushalten und dort mit Handy oder PC bereits in den meisten Kinderzimmern. Dabei ist den wenigsten bekannt, wie und wo ihre Daten tatsächlich verarbeitet werden, z. B. im Inland oder Ausland. Das aber kann für den Schutz ihrer Daten von zentraler Bedeutung sein.

Schauen wir beispielhaft auf den Einkaufsvorgang: Wurde früher mit Bargeld bezahlt und wurden vielleicht noch Rabattmarken geklebt, ist es heute die EC-Karte mit elektronischem Chip, die Rabattkarte mit Magnetstreifen und demnächst der in alle Waren implantierte RFID-Chip, die zum Einsatz kommen. Wurde früher vom Käufer eine Erkundigung über die Ware noch persönlich oder zumindest vor Ort erfragt, wird eine solche Auskunft heute in der Regel von einem Callcenter erteilt, je nach Uhrzeit des Anrufs mit Sitz in Europa oder in Asien. Gehen solche Anrufe ohne Rufnummernunterdrückung raus, lässt sich leicht feststellen, von welchem Ort der Anruf erfolgt und wem der Telefonanschluss gehört. Vielleicht hat der Händler vor dem Verkauf noch eine SCHUFA-Anfrage getätigt, dann erfolgt in der Regel auch dorthin eine Rückmeldung über die Abwicklung des Geschäfts. Noch weit datenintensiver ist der Onlineeinkauf. Fazit: Schon beim einfachsten Vorgang werden an vielen Stellen elektronische Datenspuren hinterlassen.

Zur rapide zunehmenden Verbreitung der DV-Technik gesellt sich eine andere Entwicklung: Heute gibt es nicht nur mehr Technik, sie ist auch zunehmend viel leistungsfähiger, immer komplexer und zudem sind die unterschiedlichen Systeme vielfach miteinander verknüpft oder werden in einen Leistungsrahmen integriert. Gemeint ist die möglichst umfassende Vernetzung aller nur denkbaren Kommunikations- und Datenaustauschtechniken: Internet und E-Mail, Telefon- und Telefax-Dienste, Rundfunk und Fernsehen – alles soll jederzeit an jedem Ort jedermann zur Verfügung stehen und zwar immer in einer „zweigleisigen" Form: Zu jedem (passiven) Datenempfang gehört zwingend auch die Möglichkeit der aktiven Datenübermittlung. Die bislang auf einzelne Zwecke spezialisierten Kommunikationssysteme sollen zu einer einzigen digitalen Informations- und Kommunikationsplattform zusammenwachsen. Microsoft-Chef Bill Gates proklamierte vor Jahren schon den „Informationshighway", jetzt stehen auch die dafür erforderlichen komplexen Endgeräte zur Verfügung.

Voraussetzung dafür war und ist, dass die Endgeräte zu immer größeren „Alleskönnern" werden. Das Handy zum Beispiel ist nicht mehr nur Telefon, sondern kann auch Faxe, Bilder oder Videosequenzen senden, ist Fotoapparat, Videokamera, elektronischer Terminkalender und Radio, zeigt Filme und Fernsehen, verfügt über Internettauglichkeit mit vielfältigen Funktionen, kann gleichzeitig auch noch Navigator und vieles mehr sein. Diese Geräte werden in der Regel so ausgeliefert, dass alle Funktionen uneingeschränkt aktiviert sind. Im Internetbrowser zum Beispiel werden die zuvor aufgerufenen Internetadressen gespeichert, in der SMS-Funk-

tion nicht nur die empfangenen, sondern auch die gesendeten und sogar die gelöschten Nachrichten gespeichert; Entsprechendes gilt für die E-Mail-Funktion und die Rufnummernunterdrückung ist natürlich auch nicht aktiviert.

Diese Geräte lassen sich für den unerfahrenen Einzelnen meistens nur schwer bändigen. Nicht nur, dass die Menüstruktur oft datenschutzfreundliche Einstellungen erschwert, auch die Funktionen sind oft so rudimentär, dass sich zum Beispiel Dateninhalte in Verzeichnissen nur einzeln löschen lassen, obwohl die Nutzenden gern den Inhalt des ganzen Verzeichnisses gelöscht hätten. Einige Daten werden auf der SIM-Karte, andere auf dem Festspeicher im Handy, dritte in einem zusätzlichen Mobilspeicher (beispielsweise MiniSD-Karte) gespeichert. Wer ein solches Gerät etwa nach einem Jahr Gebrauch weitergeben will, hat seine liebe Mühe, alle persönlichen Daten zu löschen. Mit dem Ausbau der SIM-Karte allein ist es jedenfalls nicht getan. Irgendetwas wird dabei immer vergessen, und seien es die eingetragenen Geburtstage im Organizer.

Warum mache ich eine solche Aufzählung, die sich übrigens noch beliebig verlängern ließe und die nicht nur für das Handy gilt, sondern entsprechend zugleich für viele andere Geräte? Nun, weil sich daran gravierende Mängel der jetzigen technischen Entwicklung festmachen lassen:

— Die voreingestellten Konfigurationen sind oft ohne Sinn für Datenschutz auf maximale Kommunikationsmöglichkeiten ausgerichtet.

— Die Anforderungen, die die Produktautomatisierung an die Nutzenden stellt, sind sehr hoch. Letztere sind für einen sachgemäßen Umgang nicht adäquat ausgebildet oder unterrichtet und, was die Datenschutzgefahren betrifft, oft ahnungslos.

— Einfache technisch unterstützte Datenschutzfunktionen wie „löschen“ oder „unterdrücken“ werden oft nicht oder nicht hinreichend mitentwickelt, viele Anbieter stellen ihren Kunden keinen ausreichenden Basisschutz zur Verfügung.

— Nicht geregelte Marktmechanismen führen dazu, dass Geräte oft nicht ausreichend getestet und daher mit Sicherheitslücken ausgeliefert werden. Der Endverbraucher wird zum Versuchskaninchen und muss sich beispielsweise selbst durch Updates um die Sicherheit seiner Geräte kümmern.

— Hinzu kommt, dass, bedingt durch die Multifunktionalität der Geräte, bei einzelbestimmter, nicht verändernder Kennung sich noch viel einfacher umfassende Profile bilden lassen.

Ergebnis: Es entstehen alltägliche Datenspuren, die wir ungewollt, unbemerkt und damit größtenteils unwissend hinterlassen. Einen Teil dieser Entwicklung habe ich genauer und ausführlicher in meinem Projekt „Profile“ auf meiner Homepage beschrieben (vgl. Ziff. 1.3 dieses Berichts). Eine der großen gesellschaftlichen Herausforderungen zur Einlösung des Rechts auf informationelle Selbstbestimmung ist die Bändigung dieser Technik, ohne sie dabei in ihrer Entwicklung zu behindern. Es kann nicht allein Aufgabe des Bundesverfassungsgerichts sein, immer wieder von der Verfassung verbriefte Grundrechte vor informationstechnisch basierten Eingriffen zu sichern. Die technischen Entwicklungen aller IT-Systeme sind künftig daran zu messen, ob das neu abgeleitete „Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme“ in angemessener Weise umgesetzt wurde. Eine Schwerpunktaufgabe der Datenschutzbeauftragten von Bund und Ländern wird es sein, diesem neuen Grundrecht Wirkung zu verschaffen und dessen Umsetzung zu kontrollieren. Es ist daher notwendig, dass mit Politik und Wirtschaft ein breiter Dialog über diese Fragen entsteht.

Das geltende Datenschutzrecht liefert für verschiedene Probleme der Entwicklung in den letzten Jahren nur sehr eingeschränkte Lösungen. Schon bei der Betrachtung des komplexen Systems der elektronischen Gesundheitskarte stößt man schnell an die Grenzen geltenden Rechts, gleiches gilt für neue Produkte wie „digitale Straßenansichten“ oder die Kommunikationsplattformen der sogenannten „Sozialen Netzwerke“. Erst recht gilt dies für die oben beschriebenen technischen Entwicklungen, die unter anderem mit Begriffen wie „Informationshighway“, „Konvergenz der Systeme“, „Ubiquitous Computing“, „RFID“, „Location Based Services“ oder „Smart Dust“ beschrieben werden. Die datenschutzrechtlichen Begriffe wie „Herr der Daten“ oder „verantwortliche Stelle“ lassen sich nicht mehr klar definieren,

allenfalls mit den Geboten der „Datensparsamkeit“ oder der „Datenvermeidung“ lässt sich hier noch ein Stück weit operieren. Der überwiegende Teil der Datenschützer ist sich daher einig, dass das geltende Recht den technischen Entwicklungen angepasst werden muss.

Ich habe zusammen mit den Datenschutzbeauftragten des Bundes und der Länder hierauf verschiedentlich hingewiesen (vgl. Ziff. 20.3 dieses Berichts) und auch meine Bereitschaft erklärt, an konstruktiven Lösungen mitzuwirken. Anders als das Bundesverfassungsgericht können aber die Datenschutzbeauftragten nicht aus der Verfassung neue Grundrechte entwickeln oder, wie der Gesetzgeber, neues Recht kreieren; sie sind an das geltende Recht gebunden, auch eine verfassungsrechtlich gebotene moderne Auslegung hat dabei ihre Grenzen.

Gleichwohl muss ich mich nicht auf eine bloße Rechtsanwendung beschränken. Vielmehr sehe ich es auch als meine Aufgabe, den Gesetzgeber auf Entwicklungen hinzuweisen, die zur Gewährleistung eines effektiven Datenschutzes einer Korrektur bedürfen (vgl. Ziff. 20.3 dieses Berichts). Die seit Jahren angemahnten Regelungen gegenüber dem Bund für einen Arbeitnehmerdatenschutz sind ein Beispiel dafür, die jüngst gemachten Vorschläge zum Adresshandel ein anderes. Für die in diesem Artikel beschriebenen technischen Entwicklungen gibt es allerdings keine rechtlichen Patentlösungen. Notwendig ist daher eine breite Diskussion, die die verschiedenen, zum Teil konkurrierenden gesellschaftlichen Ziele formuliert. Erst dann kann damit begonnen werden, die hierfür erforderlichen Rahmenbedingungen zu schaffen. Die Fortentwicklung des Rechts ist dabei ein Schritt.

Aber auch – wie es so schön heißt – der Faktor Mensch muss Berücksichtigung finden. Die Technik darf nicht zu viel von ihm verlangen. Schon jetzt muss sich Untersuchungen zufolge jeder Bundesbürger zwischen sechs und acht Passwörter oder PIN merken. In den nächsten Jahren wird sich die Zahl auf durchschnittlich zwölf erhöhen. Das überfordert viele und führt zu neuen Sicherheitslücken. Zu berücksichtigen ist dabei, dass manche Karten, die nur mit einer PIN einsatzfähig sind, lediglich einmal im Jahr oder weniger zum Einsatz kommen. Hier sind sichere und intelligente Lösungen gefragt. Auch die Menüführung komplexer IT-Geräte sollte ein eigenes Feature „Datenschutz“ haben.

Viele Sicherheits- und Datenschutzprobleme bei IT-Produkten sind – wie oben skizziert – auf unsichere Grundeinstellungen der Systeme zurückzuführen. So wurden vor nicht allzu langer Zeit noch WLAN-Komponenten zunächst ohne, später ohne aktivierte Verschlüsselungsfunktion ausgeliefert. Dem Normalanwender war es daher nicht oder nur unter Schwierigkeiten möglich, einen sicheren Betrieb seines WLAN (Funknetz zum Internet) zu gewährleisten. Hacking, unzulässigen Downloads und Datenmissbrauch wurden damit Tür und Tor geöffnet. So hat denn auch eine im Auftrag von Frontal21 durchgeführte Untersuchung ergeben, dass bei bis zu 45 % von ca. 4000 in Deutschland überprüften DSL-Anschlüssen die Rechner direkt über eine öffentliche IP-Adresse erreichbar waren, also per DSL-Modem ungeschützt an das Internet angebunden waren. Eine rechtliche Handhabe zur Erzwingung technischer Sicherheit für die Käufer gab und gibt es aber nicht. Wichtig ist daher, dass die Hersteller und die für den Betrieb der Systeme verantwortlichen Unternehmen verpflichtet werden können, für eine sichere technische Grundausstattung zu sorgen.

Zugleich muss ein Wettbewerb entstehen, verständliche Benutzungshinweise und einfach zu bedienende Hard- und Software für die Anwender zu erstellen. Es muss möglich sein, auf einfache Weise ein für die eigenen Daten angemessenes Schutzniveau einstellen zu können. Die Hersteller von informationstechnischen Systemen müssen für Aufklärung sorgen, damit für den Einzelnen auch klar ist, welche Datenverarbeitungsprozesse im Hintergrund ablaufen. Nur wenn diese nachvollziehbar sind, kann der Einzelne beurteilen, ob er dies in Kauf nehmen will oder nicht. Die Anbieter müssen die Nutzer auch darüber informieren, welche Risiken mit der Nutzung von informationstechnischen Geräten oder der Inanspruchnahme von elektronischen Dienstleistungen verbunden sind. Eine umfassende Information und Beratung tragen dazu bei, Transparenz zu schaffen. Transparenz ist aber eine Voraussetzung für die eigenverantwortliche Wahrnehmung der informationellen Selbstbestimmung.

Eines ist unstreitig: Die Informations- und Kommunikationstechnik birgt das Potenzial zu einer totalen Überwachung. An immer mehr Stellen werden immer mehr Daten über uns gesammelt. Damit einhergehen eine zunehmende Überwachung,

Registrierung, Bewertung sowie eine zum Teil unterschwellige Steuerung der Betroffenen. Die Rede ist hier nicht vom Überwachungsstaat, sondern von der „Überwachungsgesellschaft". Diese Entwicklung ist aber weder unausweichlich noch steht sie mit einer freiheitlich verfassten Gesellschaft im Einklang. Datenschutz ist nicht einfach bloß der Schutz von Daten, sondern der Schutz der informationellen Selbstbestimmung. Ein guter Datenschutz ist damit ein Garant für eine verfassungskonforme Informationsgesellschaft, die den Menschen im Vordergrund sieht und die Technik als ein Instrument zur Unterstützung seiner freien und selbstbestimmten Entfaltungsmöglichkeiten. Auch das gehört zum Schutz unserer verfassungsmäßigen Ordnung und solange die technische Entwicklung sich nicht selbst ausreichend in die Pflicht nimmt, muss die Gesellschaft für Erhalt oder Einführung notwendiger Rahmenbedingungen Sorge tragen.

1.6 Datenschutzrechtliche Gesetzesinitiativen

In Zentrum der Weiterentwicklung datenschutzrechtlicher Bestimmungen steht im Berichtsjahr nicht der öffentliche Bereich, auch wenn es hier z. B. durch die Änderungen im BKA-Gesetz oder im Personalausweisgesetz durchaus bemerkenswerte Weichenstellungen gegeben hat.

Auskunfteien-Regelungen: Ende Juli hat das Bundeskabinett einen Gesetzentwurf beschlossen, mit dem das Bundesdatenschutzgesetz (BDSG) um Regelungen zur Auskunfteientätigkeit ergänzt werden soll (BT-Drs. 16/10529). Neben der Schaffung eines spezifischen Erlaubnistatbestands für Datenübermittlungen an Auskunfteien ist dabei die erstmalige Regelung zum sogenannten Scoringverfahren von zentraler Bedeutung. Dabei handelt es sich um ein mathematisch-statistisches Verfahren zur Berechnung eines Zahlwertes, der Auskunft darüber gibt, mit welcher Wahrscheinlichkeit der Betroffene seinen finanziellen Vertragspflichten nicht nachkommen kann. Hierzu werden nicht nur Angaben über das tatsächliche Zahlungsverhalten sowie die Einkommens- und Vermögensverhältnisse der jeweils Betroffenen – soweit verfügbar – einbezogen, sondern auch soziodemographische Daten wie Alter, Wohnumfeld oder von Dritten angekaufte oder aus allgemein zugänglichen Registern entnommene Daten, wie zum Beispiel Kfz-Daten des Kraftfahrzeugbundesamtes. Auf der Grundlage dieses vielschichtigen Zahlenmaterials wird die Bonität des Einzelnen bewertet. Dem Betroffenen wird damit die Möglichkeit genommen, allein durch rechtstreues Verhalten sein Erscheinungsbild gegenüber Vertragspartnern zu beeinflussen. Insbesondere die Einbeziehung soziodemographischer Daten birgt die Gefahr, dass über den Betroffenen ein falsches Bild mit erheblichen nachteiligen Auswirkungen für die Bonitätswertberechnung entsteht. Für den Betroffenen muss daher wenigstens klar sein, welche Informationen mit welcher Gewichtung in einen Scorewert eingeflossen sind, nur so kann er bei einem negativen Scorewert ggf. Korrekturen anbringen. Der Gesetzentwurf sieht daher vor, dass die Informations- und Auskunftsrechte der Betroffenen ausgebaut werden.

Adresshandel-Regelungen: Nach dem sog. Datenschutzgipfel und vielem Hin und Her hat Anfang Dezember des Berichtsjahres die Bundesregierung reagiert und neben dem vorgenannten Gesetzentwurf einen weiteren Gesetzentwurf zur Änderung der Regelungen zum Adresshandel auf den Weg gebracht (BT-Drs-Nr. 4/09). Mit der Novellierung des Bundesdatenschutzgesetzes will die Bundesregierung aus den jüngst bekannt gewordenen Datenschutzverstößen im Bereich der Privatwirtschaft die Konsequenzen ziehen. Die uneingeschränkte Streichung des Listenprivilegs und die Pflicht zur Einholung einer Einwilligung des Betroffenen bei der Übermittlung seiner Daten an Dritte oder bei der Nutzung für Werbezwecke für Dritte sind erforderlich, um das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger zu stärken. Das habe ich sowohl mit der Konferenz der Datenschutzbeauftragten (vgl. Ziff. 20.10 dieses Berichts) wie auch mit den obersten Aufsichtsbehörden für den Datenschutz (vgl. Ziff. 21.5 dieses Berichts) in Entschließungen bzw. Beschlüssen angemahnt. Der Gesetzentwurf der Bundesregierung trägt dem allerdings nur bedingt Rechnung, löst zudem weitere Forderungen der Datenschützer, wie die Verbesserung der Protokollierung des Datenzugriffs in automatisierten Verfahren oder die lückenlose Dokumentation der Herkunft der Daten, nicht ein.

Arbeitnehmerdatenschutz-Regelungen: Medienberichten zufolge beschäftigen sich in den Betrieben mittlerweile ganze Abteilungen mit dem Aufspüren, Analysieren und Auswerten von Protokolldateien. Es ist bekannt, dass durch den Einsatz von

Videotechnik, durch die elektronische Überwachung des E-Mail-Verkehrs und des Surfverhaltens, durch funk- oder biometriegesteuerte Zugangssysteme, durch Skill-Datenbanken und vieles mehr, Arbeitnehmer immer mehr einer feinmaschigen Kontrolle und Überwachung ausgesetzt sind. Die modernen informationstechnischen Systeme ermöglichen eine immer größere Überwachungsdichte, wobei die bislang zielgerichtete Überwachung von Arbeitnehmern zunehmend ungezielt und zeitlich wie räumlich allgegenwärtig wird. Dabei erfolgt sie häufig so subtil, dass sie von den Betroffenen weder in Art noch in Umfang erkannt wird. Rechtliche Regelungen sind zum Teil gar nicht oder nur verstreut an verschiedenen Regelungsorten vorhanden und wurden, was vielen Beschäftigten nicht bekannt ist, zum Teil erst durch Rechtsprechung ergänzt. Nach den derzeitigen Regelungen und der Rechtsprechung des Bundesarbeitsgerichts ist eine verdeckte Überwachung von Beschäftigten, sei es mit Videokameras, Überwachungssoftware o. ä., grundsätzlich nicht zulässig, weil sie deren Persönlichkeitsrecht erheblich verletzt. Viele Beschäftigte kennen ihre Rechte nicht und eine Kontrolle der Einhaltung bestehender Regelungen durch z. B. betriebliche Datenschutzbeauftragte findet oft nicht statt. Ich brauche dafür gar nicht auf den Fall Lidl zurückgreifen, meine Berichte der letzten Jahre unter der Rubrik „Videoüberwachung“ enthalten genügend Belege für diese Tendenzen. Wenn Beschäftigte von derartigen Überwachungen etwas erfahren, wenden sie sich sehr häufig nicht an mich, weil sie Angst davor haben, ihren Arbeitsplatz zu verlieren oder sonst im Betrieb benachteiligt zu werden. Es ist daher zu begrüßen, dass jetzt neben der seit Jahren bestehenden Aufforderung des Bundestages, gesetzliche Arbeitnehmerdatenschutzregelungen zu erarbeiten, durch eine Bundesratsinitiative erneut Bewegung in die Sache gekommen ist (BR-Drs. 665/08). Sie kommt allerdings wohl im Bund zu spät für diese Legislaturperiode.

1.7 Wenn das mal seine Adresse war . . .

„Adressen, Adressen, Adressen, ich will, doch ich kann keine vergessen“, so mag der Computer einer Auskunftei programmiert gewesen sein, als er als Vor-Voradresse die Anschrift der JVA in Bremen auswies und deshalb der ehemalige Strafgefangene eine unbedingt benötigte behindertengerechte Wohnung nicht bekam. Auch die unter der in den USA geführten Internetseite „Rotten Neighbor“ könnte durchaus für Mietsuchende nachteilige Auswirkungen haben. Dort sind zum Teil widerwärtige Informationen über eine Vielzahl Bremer Bürger hinterlegt (Näheres vgl. Ziff. 4.6 dieses Berichts). Jüngere Stimmen in der Literatur meinen, Privatheit und auch das damit verbundene informationelle Selbstbestimmungsrecht seien Relikte des zwanzigsten Jahrhunderts. Dem ist zu entgegnen: Auch unsere Verfassung ist aus dem vergangenen Jahrhundert, ja, und sie ist auch mit Blick auf die sich verändernden gesellschaftlichen Umstände immer wieder neu zu interpretieren, aber ein Verzicht auf diese Werte kommt wohl nicht infrage. Die Kontrolle über die als „eigene Bereiche“ eingestuften Angelegenheiten ist nicht nur in der eigenen Wohnung, sondern auch – wie der Fall des Mietsuchenden zeigt – im Bereich der personenbezogenen Daten außerordentlich wichtig.

2. Betriebliche und behördliche Beauftragte für den Datenschutz

2.1 Behördliche Beauftragte für den Datenschutz

Die behördlichen Datenschutzbeauftragten haben wichtige Aufgaben wahrzunehmen, deren Bedeutung bei einer immer umfangreicher und komplexer werdenden Datenverarbeitung stetig zunimmt. Gerade die behördlichen Datenschutzbeauftragten sind es, die in ihren Dienststellen eine besondere Verantwortung für die Sicherstellung und Gewährleistung eines angemessenen Datenschutzniveaus tragen. Die Umsetzung der gesetzlichen Anforderungen ist häufig nicht leicht und mit ganz unterschiedlichen Problemen technischer und rechtlicher Art verbunden. Um ihnen die Wahrnehmung ihrer Aufgaben zu erleichtern und sie zu unterstützen, sind im Frühjahr und Herbst des Berichtsjahres mit den behördlichen Datenschutzbeauftragten wieder Workshops durchgeführt worden, wobei die Veranstaltung im Frühjahr im Aus- und Fortbildungszentrum der bremischen Verwaltung stattgefunden hat. Mit der Art der Durchführung der Workshops und den darin behandelten Schwerpunktthemen habe ich dabei versucht, den Praxisbezug der Workshops noch weiter zu verbessern.

Nicht nur in Bremen, sondern auch beim Bund und in anderen Ländern, wie z. B. Niedersachsen, gibt es behördliche Beauftragte für den Datenschutz. Die von den

Datenschutzbeauftragten wahrzunehmenden Aufgaben sind durchaus vergleichbar. Ihre Aufgabe ist es insbesondere, auf die Einhaltung der datenschutzrechtlichen Vorschriften in ihren Behörden hinzuwirken. Für den Workshop im Frühjahr des Berichtsjahrs ist es mir gelungen, zwei bereits seit mehreren Jahren im Umland Bremens tätige und sehr engagierte kommunale Datenschutzbeauftragte aus dem Landkreis Diepholz und aus Oldenburg für Vorträge und Diskussionsrunden zu gewinnen. Im Workshop haben die beiden die teilnehmenden Datenschutzbeauftragten aus der bremischen Verwaltung ausführlich über ihre Ideen, Vorgehensweisen und Erfahrungen in der Verwaltungspraxis informiert.

In einem Vortrag über die Arbeit eines behördlichen Datenschutzbeauftragten hat der Datenschutzbeauftragte des Landkreises Diepholz insbesondere über seine Tätigkeit im Netzwerk der kommunalen Datenschutzbeauftragten in der Region NORDWEST und in der Kreisverwaltung berichtet. Bereits seit mehreren Jahren treffen sich die behördlichen Datenschutzbeauftragten der Kommunen in der Region NORDWEST regelmäßig. Von Cuxhaven bis Osnabrück, von Emden bis Nienburg arbeiten die Datenschützer in einem Netzwerk eng zusammen und unterstützen sich gegenseitig. Die datenschutzrechtlichen Probleme in den Kreis- und Rathäusern sind häufig die gleichen. Die Datenschutzbeauftragten erarbeiten deshalb gemeinsam Lösungen, die sie in ihren Verwaltungen umsetzen. Gemeinsame Veranstaltungen werden selbst organisiert und bieten eine gute Möglichkeit, Synergieeffekte zu erzielen und den Datenschutz voranzubringen.

Im Hinblick auf die Tätigkeit beim Landkreis Diepholz hat dessen Datenschutzbeauftragter die Teilnehmer des Workshops insbesondere über die Entwicklung eines Datenschutzmanagementsystems und den damit verbundenen Aufbau eines Kompetenzzentrums Datenschutz, Schulungen der Mitarbeiterinnen und Mitarbeiter der Kreisverwaltung, die Bedeutung der Öffentlichkeitsarbeit für die Wahrnehmung der Aufgaben des behördlichen Datenschutzbeauftragten und seine Funktion als Dienstleister in Sachen Datenschutz im Kreishaus informiert.

Der Datenschutzbeauftragte der Stadt Oldenburg hat die teilnehmenden Datenschutzbeauftragten in einem Vortrag zum Thema „RFID – Fluch oder Segen“ über Gefahren und Risiken des Einsatzes von RFID-Systemen unterrichtet und auf die Aufgaben und die Bedeutung hingewiesen, die die Datenschutzbeauftragten im Hinblick auf die Begleitung der Einführung neuer technischer Systeme in der Verwaltung haben.

Die Berichte der Datenschutzbeauftragten aus dem niedersächsischen Umland Bremens sind bei den Teilnehmern des Workshops auf erhebliche Resonanz gestoßen. Gerade auch für ihre eigene Arbeit haben sie sehr interessante Anregungen erhalten. Bei den sich an die Vorträge anschließenden Diskussionsrunden haben alle Teilnehmer die Gelegenheit zum Austausch der bei ihrer Tätigkeit gesammelten Erfahrungen erhalten, wovon reger Gebrauch gemacht worden ist.

Schwerpunkt des Workshops im Herbst des Berichtsjahrs, der ebenfalls bei den Teilnehmern auf starke Resonanz gestoßen ist, ist das Thema „Datenschutzmanagement in den Dienststellen der bremischen Verwaltung“ gewesen. Bei der Gestaltung und Organisation des Datenschutzes in den Behörden werden an die behördlichen Datenschutzbeauftragten die unterschiedlichsten Fragestellungen gerichtet. Dies erfordert neben umfassenden Kenntnissen der zu gewährleistenden rechtlichen und technischen Anforderungen auch ein umfangreiches Wissen, wie die Anforderungen in den jeweiligen Dienststellen umgesetzt werden können. Von Bedeutung sind dabei insbesondere die Gestaltung der innerorganisatorischen Abläufe, die Möglichkeiten der Sensibilisierung von Mitarbeiterinnen und Mitarbeitern für Datenschutzfragen und die Einbindung der Datenschutzbeauftragten in den Behörden. Nach umfassenden Vorträgen zum Thema und anschließender Diskussion war auch wieder Gelegenheit zum Erfahrungsaustausch gegeben, wovon erneut reger Gebrauch gemacht worden ist.

Die Reihe der Workshops soll im nächsten Jahr mit weiteren aktuellen ressortübergreifenden Themen fortgesetzt werden. Unterstützung für die Wahrnehmung ihrer Tätigkeit gebe ich den behördlichen Datenschutzbeauftragten darüber hinaus auch weiterhin durch mein Internetangebot mit auf diese Tätigkeit speziell abzielenden Beiträgen der behördlichen Datenschutzbeauftragten. Anrufe wie auch die Workshops zeigen, dass die Erfüllung in den Dienststellen weiterhin mit Konflikten verbunden ist. Zum Beispiel ist das Problem aufgetreten, dass die behördliche Datenschutzbeauftragte einer bremischen Behörde gleichzeitig mit der Leitung ei-

nes DV-Projektes betraut wurde, das der Entwicklung eines Verfahrens dient, bei dem auch personenbezogene Daten verarbeitet werden. Grundsätzlich sind diese beiden Funktionen, die Wahrnehmung der Aufgaben der Projektleitung und der Datenschutzbeauftragten in Personalunion – wie in diesem Fall – mit § 7 a BremDSG unvereinbar. Danach muss die behördliche Datenschutzbeauftragte bzw. der behördliche Datenschutzbeauftragte die erforderliche Zuverlässigkeit und Unabhängigkeit zur Ausübung seiner datenschutzrechtlichen Kontrolle besitzen. Liegen die Funktionen der Projektleitung und des Datenschutzes aber wie hier in einer Person, ist eine solche Kontrolle nicht möglich, so dass ein Rollenkonflikt divergierender Interessen besteht. Eine Splittung von Projektleitungsfunktion und Datenschutzfunktion ist sicherzustellen. Eine Stellungnahme des Justizressorts bestätigt meine Auffassung.

2.2 Betriebliche Beauftragte für den Datenschutz

Wie schon in den letzten Jahren habe ich auch 2008 regelmäßig die Sitzungen des Erfa-Kreises der GDD begleitet. Hier treffen sich betriebliche Datenschutzbeauftragte und tauschen sich über Probleme und aktuelle Ereignisse aus. Für mich als Aufsichtsbehörde ist es immer wieder interessant zu verfolgen, welche Datenschutzthemen gerade in der Wirtschaft auf der Tagesordnung stehen. In diesem Jahr wurde u. a. eine Orientierungshilfe zur datenschutzgerechten Entsorgung vorgestellt, der stellvertretende Geschäftsführer der GDD berichtete über die aktuellen Entwicklungen im Datenschutz, Datenschutzdienstleister präsentierten sich, und über die Notwendigkeit eines Arbeitnehmerdatenschutzgesetzes wurde diskutiert. Darüber hinaus waren die diversen Datenschutzskandale ein Thema.

3. Datenschutzaudit

3.1 Entwurf des Bundes zur Regelung des Datenschutzaudits

Das Bundesministerium des Innern hat im Berichtsjahr gemeinsam mit dem Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes (BDSG) den Entwurf eines Gesetzes zur Regelung des Datenschutzaudits (Datenschutzauditgesetz) vorgelegt. Nach Maßgabe dieses Gesetzes sollen verantwortliche Stellen ihr Datenschutzkonzept und Anbieter von Datenverarbeitungsanlagen und -programmen die von ihnen angebotenen informationstechnischen Einrichtungen kontrollieren lassen können, sofern sie nicht öffentliche Stellen im Sinne des Bundesdatenschutzgesetzes sind. Sie sollen bei Vorliegen der erforderlichen Voraussetzungen die Möglichkeit erhalten, ihr Datenschutzkonzept oder eine angebotene informationstechnische Einrichtung mit einem Datenschutzauditsiegel zu kennzeichnen. Nach einem umfangreichen und sehr komplizierten Regelwerk des Datenschutzauditgesetzes sollen die für die Auditierung erforderlichen Kontrollen durch private Kontrollstellen durchgeführt werden, die der Aufsicht der jeweils zuständigen Landesbehörde unterstehen. Darüber hinaus soll beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ein Datenschutzauditausschuss gebildet werden, der Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit erlässt.

Der vorgelegte Gesetzentwurf genügt nicht den Anforderungen, um Verbesserungen für den Datenschutz und die Datensicherheit zu erreichen (vgl. 30. JB, Ziff. 3.2). Nach den von mir in Bremen mit der Durchführung von Datenschutzauditierungen im öffentlichen Bereich gewonnenen Erfahrungen ist eine sinnvolle Beurteilung von Produkten nur in ihrer technischen Umgebung und ihrem konkreten Einsatzbereich sinnvoll (Verfahrensaudit). Nach dem Entwurf kann jedoch auch ein abstraktes, hiervon unabhängiges Produktaudit bei den Anbietern von Datenverarbeitungsanlagen und -programmen durchgeführt werden. Dabei besteht die Gefahr, dass man meint, mit dem Einsatz eines auditierten Produktes habe man alles für den Datenschutz getan. Darüber hinaus bedarf es einer konkreten Bestellung von Sachverständigen für einzelne Verfahren. Es gibt nach meiner Einschätzung keine Sachverständigen, die eine Allroundeignung haben für jedwedes technische Verfahren. Der Gesetzentwurf stellt diese Anforderungen an die fachliche Eignung des Personals der Kontrolleure nicht.

Der Gesetzentwurf ist ein „bürokratisches Monster“. Er ist nicht geeignet, den Datenschutz in der Wirtschaft zu verbessern, was auch der Düsseldorfer Kreis mit seinem Beschluss in der Sitzung am 13./14. November 2008 zum Ausdruck bringt (vgl. Ziff. 21.5 dieses Berichts).

3.2 Datenschutzaudit nach § 7 b BremDSG

Im Berichtsjahr wurde kein Verfahren nach dieser Vorschrift auditiert.

4. Internet, Telekommunikation, Teledienste

4.1 Prüfung von Onlineshops

Im Sommer dieses Jahres habe ich die Verarbeitung personenbezogener Nutzerdaten in drei Onlineshops geprüft. Es handelte sich hierbei um eine zweistufige Prüfung. Ich habe zunächst den Onlineshops einen umfassenden Fragenkatalog mit der Bitte um Beantwortung übersandt. Hier wurden u. a. das Verfahren, welches die Nutzer bei Abschluss eines Vertrages durchlaufen müssen, der Umgang mit Bestandsdaten, die Verarbeitung und Nutzung von Daten für Werbezwecke, die Erstellung von Nutzungsprofilen, das Setzen von Cookies sowie die Gewährleistung der Datensicherheit abgefragt. Im zweiten Schritt habe ich dann die Verfahren vor Ort in Augenschein genommen.

Bei einem der geprüften Onlineshops war die Umsetzung aus datenschutzrechtlicher Sicht vorbildlich. Es konnten fast keine Mängel festgestellt werden. Lediglich eine Klausel in der Datenschutzerklärung musste überarbeitet werden. Es fiel insbesondere positiv auf, dass die Kunden ausschließlich gegen Rechnung bestellen konnten und damit keine Kontoverbindungsdaten übermittelt werden mussten. Außerdem ermöglichte das System, die komplette Nutzung des Shops in verschlüsselter Form.

Demgegenüber habe ich gegenüber einem anderen Onlineshop die nicht vorhandene Verschlüsselung bei der Übertragung personenbezogener Daten bemängeln müssen. Aber auch dieser Shop genügte im Übrigen den datenschutzrechtlichen Anforderungen im vollen Umfang.

Die Prüfung eines weiteren Shops erwies sich aus datenschutzrechtlicher Sicht kritischer. So nutzte das Unternehmen zur Abwicklung der Aufträge weitere Onlinesysteme, die mit dem eigentlichen Shopsystem – teils automatisiert – Daten austauschten. Das Unternehmen konnte bisher nicht darlegen, dass dieser Datenaustausch in verschlüsselter Form geschieht. Weiterhin wurden durch das Unternehmen halbautomatisch die Daten von Zahlungseingängen auf dem Firmenkonto des Unternehmens an das Auftragsabwicklungssystem transferiert, wodurch auch Kontoverbindungsdaten von Kunden aus dem Haus gegeben wurden, ohne dass diese davon Kenntnis erlangten, also auch Bankverbindungsdaten von Kunden, die bewusst per Rechnung und manueller Überweisung zahlen, plötzlich auf Servern im Internet lagern. Aufgrund der Komplexität der eingesetzten Systeme ist die Prüfung noch nicht vollständig abgeschlossen und bedarf noch weiterer Sachverhaltsaufklärungen.

4.2 Internetportale zur Bewertung von Einzelpersonen

Die Anzahl der Portale zur Bewertung von einzelnen Personen (Lehrer, Ärzte, Handwerker, Nachbarn etc.) nimmt rapide zu. So können z. B. bei www.spickmich.de Lehrer und bei www.meinprof.de Professoren bewertet werden. Auf einer anderen Internetseite waren 300 000 Ärzte und Heilberufler gelistet. Patienten konnten diese in fünf Bereichen mit vier unterschiedlichen Notenstufen bewerten. Ein Bereich betraf z. B. die Wartezeiten. Diese Veröffentlichungen sind aus datenschutzrechtlicher Sicht nicht unbedenklich, weil sie einen erheblichen Eingriff in das Persönlichkeitsrecht der Betroffenen darstellen. Zudem ermöglichen sie es den Bewertern, unter dem Deckmantel der Anonymität Meinungsäußerungen über die Betroffenen kundzutun, die sie bei Offenlegung ihrer Identität so evtl. nicht tätigen würden.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich haben diese Entwicklung zum Anlass genommen und in einem Beschluss zu „Internet-Portalen zur Bewertung von Einzelpersonen“ insbesondere auf die jederzeitige Abrufbarkeit der Bewertungen, die oftmals sensible Informationen darstellen, hingewiesen. Bei der nach dem Bundesdatenschutzgesetz (BDSG) vorgeschriebenen Abwägung muss den schutzwürdigen Interessen der bewerteten Person Rechnung getragen werden. Das Recht auf freie Meinungsäußerung rechtfertigt nicht das Recht der Bewerteten auf informationelle Selbstbestimmung als nachrangig zu beurteilen (Näheres vgl. Ziff. 21.1 dieses Berichts).

4.3 Strafbarkeit der Nutzung eines offenen WLAN

Das Amtsgericht Wuppertal hat in einem neueren Urteil (Az. 22 Ds 70 Js 6906/06) entschieden, dass die Nutzung eines offenen Zugangs zu einem WLAN ein strafbares Abhören von Nachrichten sowie ein Verstoß gegen die Strafvorschriften des Bundesdatenschutzgesetzes (BDSG) darstellt. Der Verstoß gegen das Datenschutzrecht liegt nach Auffassung des Gerichts darin, dass sich der Täter die IP-Adresse des Routers verschafft hat. Diese sei ein nicht allgemein zugängliches personenbezogenes Datum. Für die zur Verwirklichung des Straftatbestandes erforderliche Bereicherungs- bzw. Schädigungsabsicht komme es auch nicht darauf an, ob der WLAN-Betreiber eine Flatrate habe. Vielmehr nehme man bei Nutzung eines WLAN zumindest billigend in Kauf, dass der WLAN-Betreiber über keine Flatrate verfüge und damit seinen Internetanschluss nach Volumen oder Zeit abrechnen müsse.

4.4 Veröffentlichung der Daten eines Fanclub-Verantwortlichen

Im Februar beschwerte sich ein Fanclub-Verantwortlicher bei mir, dass seine privaten Daten (Anschrift, private E-Mail) ohne Einholung seiner Einwilligung auf der Homepage eines bekannten Bremer Vereins veröffentlicht worden seien. Die Veröffentlichung führte dazu, dass der Eingeber eine Flut von Werbezusendungen, elektronisch wie auch auf dem Postwege, erhielt. Nach Schilderung des Betroffenen war der Verein seiner mehrmaligen Aufforderung, die Daten von der Homepage zu nehmen, nicht nachgekommen. Daher schrieb ich den Verein an und teilte ihm mit, dass für die Veröffentlichung personenbezogener Daten im Internet grundsätzlich die Einwilligung der Betroffenen erforderlich ist. Daraufhin wurden die Daten des Fanclub-Verantwortlichen von der Homepage des Vereins genommen.

4.5 Datenschutz in sozialen Netzwerken

Soziale Netzwerke im Internet, wie studiVZ, schülerVZ oder xing, verzeichnen einen enormen Zulauf. Man geht davon aus, dass die Hälfte der Internetnutzer regelmäßig soziale Netzwerke besucht. So verzeichnete z. B. studiVZ im ersten Quartal 2008 sechs Millionen Besucher (Quelle: Nielsen Online).

Von den Mitgliedern wird aber oftmals übersehen, dass sie mit ihrer Anmeldung in sozialen Netzwerken und der Veröffentlichung von Informationen im Laufe der Teilnahme auch ein erhebliches Maß an Privatheit preisgeben. Die Verbreitung von zu vielen privaten bzw. sensiblen Informationen ist nicht unproblematisch. So besuchen auch potenzielle Arbeitgeber diese Foren und verschaffen sich gern einen Überblick, was der Bewerber über sich in den sozialen Netzwerken preisgibt. Die veröffentlichten Informationen der Nutzer ermöglichen eine Auswertung des dargebotenen Profils. Es ist auch nicht sichergestellt, dass die Informationen nur in der Online-Community (Gemeinschaft von Menschen, die einander via Internet begegnen und sich dort austauschen) bleiben, obwohl dieser Eindruck gern von den Betreibern vermittelt wird.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich haben sich der Datenschutzproblematik von sozialen Netzwerken angenommen und einen Beschluss zur „Datenschutzkonformen Gestaltung sozialer Netzwerke“ gefasst (vgl. Ziff. 21.2 dieses Berichts). Darin werden die Anbieter aufgefordert, u. a. folgende rechtliche Rahmenbedingungen einzuhalten: Die Nutzer sind umfassend über die Verarbeitung ihrer personenbezogenen Daten und über ihre Wahl- und Gestaltungsmöglichkeiten zu unterrichten. Eine Verwendung von personenbezogenen Daten für Werbezwecke ist nur zulässig, soweit eine wirksame Einwilligung der Betroffenen vorliegt. Die Speicherung von personenbezogenen Nutzungsdaten über das Ende der Verbindung hinaus ist ohne Einwilligung der Nutzer nur zulässig, soweit die Daten zu Abrechnungszwecken gegenüber dem Nutzer erforderlich sind. Außerdem muss auch die Möglichkeit bestehen, anonym oder pseudonym im sozialen Netzwerk zu agieren. Darüber hinaus muss es dem Nutzer ermöglicht werden, sein Profil einfach zu löschen. Schließlich müssen die Anbieter durch technisch-organisatorische Maßnahmen einen systematischen oder massenhaften Export oder Download von Profildaten aus dem sozialen Netzwerk verhindern.

4.6 Internetportal „Rotton Neighbor“

Rotten Neighbor bedeutet soviel wie „verfaulter, verdorbener, niederträchtiger Nachbar“. Um eine absurde Seite erweitert – das Wort reicher verbietet sich hier –

ist das Internet mit der in den USA betriebenen Seite „rottonneighbor“ geworden. Auf einer Landkarte bzw. einem Stadtplan werden Objekte angezeigt, zu denen Meinungsäußerungen zu dort lebenden Personen abgespeichert sind. Einige der beleidigenden Einträge habe ich im Anhang (vgl. Ziff. 23.5) beigefügt. Das Problem ist, dass viele Betroffene gar nicht wissen, dass sie dort diffamiert werden. Wer Urheber für die Einträge ist, ist darüber hinaus für alle Betroffenen nicht nachvollziehbar. Die Datenschutzbeauftragten des Bundes und der Länder können mangels Zuständigkeit nicht eingreifen. Es kann aber nicht geduldet werden, dass widerwärtige Beschimpfungen unter einem beliebigen Pseudonym veröffentlicht werden können. Die Meinungsfreiheit endet, wo Beleidigung anfängt und für mich gehört auch dazu, dass man erkennen kann, von wem diese Meinung stammt, damit man sich eine eigene Meinung darüber bilden kann. Ich finde es auch nicht hinnehmbar, wenn jeder Betroffene gegenüber einem US-Unternehmen einzeln für seine Rechte eintreten muss, vielmehr muss ihm durch das System die Möglichkeit gegeben werden, sich unmittelbar mit dem Meinungsverursacher auseinandersetzen zu können. In diesem Sinne engagiere ich mich bei den Datenschutzaufsichtsbehörden, um über die europäische Schiene etwas zu erreichen.

5. Medien

5.1 Förderung des Datenschutzbewusstseins in der jungen „Online-Generation“

Gerade Jugendliche nutzen die modernen Informationssysteme in erheblichem Umfang. Da bei ihnen das Datenschutzbewusstsein meistens noch nicht besonders ausgeprägt ist, ist es wichtig, sie über die Risiken umfassend aufzuklären. Die Datenschutzbeauftragten des Bundes und der Länder sehen es als wichtige Aufgabe an, Kinder und Jugendliche für einen sorgsamen und verantwortungsbewussten Umgang mit persönlichen Daten zu sensibilisieren und haben dies zu einer Entschließung zur „Medienkompetenz und Datenschutzbewusstsein in der jungen Online-Generation“ (vgl. Ziff. 20.8 dieses Berichts) zum Ausdruck gebracht. Neben meiner Lerneinheit „www.datenschutz4school.de“ bereite ich ein Projekt in Kooperation mit der Senatorin für Bildung und Wissenschaft vor.

5.2 Bericht aus dem Arbeitskreis Medien

Der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder tagte zweimal im Jahr 2008. Dabei waren Gegenstand der Beratungen u. a. folgende Themen: Handyortung im Notfall, Einsatz von Voice over IP in der öffentlichen Verwaltung, datenschutzrechtliche Aspekte des Urheberrechts bei der Nutzung des Internets, Google Analytics, Web 2.0. sowie die Gewährleistung des Datenschutzes bei der GEZ. Einzelheiten können gern auf Nachfrage mitgeteilt werden.

6. Datenschutz durch Technikgestaltung und -bewertung

6.1 Ganz private Daten im Internet

Im Berichtsjahr traten vermehrt Beschwerden darüber auf, dass Bürger ihre privaten Daten und Dokumente bei Recherchen im Internet finden konnten. So berichtete eine Bürgerin über ihren Lebenslauf, den sie bei einer Google-Suche gefunden habe; in einem anderen Fall gab ein Bürger an, dass er bei einer Google-Suche auf E-Mails gestoßen sei, die er vor ungefähr einem Jahr u. a. mit seinen Kontoverbindungsdaten an die Anzeigenabteilung einer Bremer Tageszeitung geschickt habe. Die Bürger sind irritiert und sehr empört darüber, dass ihre Daten im Internet auffindbar sind.

Viele Fälle konnte ich aufklären, aber nicht in allen konnte ich helfen. Einige beruhen auch auf fehlendem technischen Sachverstand. Nach Überprüfung solcher Sachverhalte konnte ich einige Bürger dahingehend beruhigen, dass die oben beschriebenen Daten nicht bei Google zu finden sind. Vielmehr hatten diese Bürger, die sich mit diesen oder ähnlichen Anfragen und Beschwerden an mich wandten, auf ihren Computern das von Google kostenlos abgegebene Software-Werkzeug „Google Desktop“ in Betrieb. Dieses Software-Werkzeug indiziert mit ähnlichen Mechanismen wie bei der „großen“ Internetsuchmaschine die vollständigen Inhalte der lokalen Datenträger des PC, auf dem es installiert ist. Dadurch sind für die Anwender die Inhalte der eigenen Datenträger mit den von Google bekannten Me-

chanismen recherchierbar. Die Inhalte der Festplatten werden nicht via Internet an Google übertragen, die Indizes verbleiben auf der lokalen Festplatte. Allerdings erfolgt die Anzeige der Suchergebnisse genau wie bei der reinen Internetsuchmaschine innerhalb eines Web-Browsers. In der Liste der Suchergebnisse tauchen die lokalen Ergebnisse in der Regel vor den Suchergebnissen aus dem Internet auf. Die kombinierte Auflistung lokaler Suchergebnisse und von Suchergebnissen aus dem Internet auf einer Bildschirmseite führt bei den Nutzern gehäuft zu Irritationen. Die von diesem Personenkreis beschriebenen Sachverhalte konnten nach kurzer Rücksprache geklärt werden. Die betroffenen Bürger äußerten in der Regel, dass sie Google Desktop im Einsatz hätten, es aber nach dieser Erfahrung wieder von ihren Systemen entfernen würden.

6.2 Datenschutzrisiko Fotokopierer

Moderne Fotokopierer sind Multifunktionsgeräte und ungeheuer praktisch: Neben der reinen Kopierfunktion können sie auch als Netzwerkdrucker und Scanner eingesetzt werden. Mit ihnen werden alle denkbaren Arten von personenbezogenen Daten verarbeitet: Bewerbungen, Gehaltsbescheinigungen, Fotos, Kontoauszüge, medizinische Berichte und Gutachten, Führungszeugnisse und Strafbefehle, Asylanträge, Liebesbriefe und -gedichte. Die Liste könnte endlos weitergeführt werden. Die Nutzer achten in der Regel darauf, dass weder Originale noch Kopien im Gerät verbleiben. Die Daten aber, die in den Speichern der Kopierer verbleiben, können in der Regel nicht einfach und problemlos von den Geräten entfernt werden. Die Daten sind noch im Festspeicher sichtbar, aber mehr nicht.

Für die einzelnen Funktionen wie Kopieren, Drucken oder Scannen müssen innerhalb der Kopierer oft riesige Datenmengen bewegt, sortiert und gespeichert werden. Die Daten von normalen Druckjobs oder Kopieraufgaben werden zumeist vorübergehend zwischengespeichert und erst nach Beendigung der Aufgabe gelöscht. Gescannte Dokumente oder Bilder bleiben wenigstens so lange abgespeichert, bis sie auf andere Computer oder Datenträger kopiert oder verschoben werden. Für diese Aufgaben sind die Geräte mit großen internen Speichern ausgestattet. Dabei handelt es sich zum einen um flüchtige Arbeitsspeicher, deren Inhalte beim Ausschalten des Geräts gelöscht werden und zum anderen um nicht flüchtige Speicher wie Festplatten, die ihre Inhalte auch dann behalten, wenn der Kopierer ausgeschaltet wird. Die nicht flüchtigen Speicher werden zum Zwischenspeichern genutzt, wenn die Datenmengen nicht direkt vom Gerät verarbeitet werden können. Nach Beendigung einer Aufgabe wird der belegte Speicherplatz zwar automatisch wieder freigegeben, die Daten aber nicht zwingend unumkehrbar gelöscht: Der Speicherplatz wird lediglich als „zum Überschreiben freigegeben" gekennzeichnet. Es verbleiben in der Regel noch Daten auf den Speichern der Kopierer. Zumindest bleibt aber immer die Unsicherheit, dass möglicherweise nicht mehr benötigte Daten innerhalb des Systems vorhanden sind. Wenn die Daten noch vorhanden sind, lassen sie sich mit geringem technischem Aufwand wieder herstellen.

Die dafür notwendigen Informationen sind im Internet zu finden. Für nahezu jedes Gerät sind die entsprechenden Zugangsdaten zu finden: Standardpasswörter, Wartungs- oder Administratorcodes, mit denen allumfassende Rechte für das Kopiersystem erhalten werden. Damit können Unbefugte alle Möglichkeiten, die das Gerät bietet, ausschöpfen, insbesondere dann, wenn die Kopierer mit dem lokalen Computernetzwerk verbunden sind. Es muss davon ausgegangen werden, dass gespeicherte Aufträge genauso wie scheinbar gelöschte, real aber noch auf den Datenträgern vorhandene Kopien, Faxe oder Ausdrucke wieder sichtbar gemacht und ausgedruckt oder auf andere Datenträger übertragen werden können. Die Integration in Computernetzwerke bedingt, dass für sie ähnliche Sicherheitsregelungen und Sicherheitseinstellungen gelten müssen wie für herkömmliche, an Netzwerke angeschlossene Computer.

Kritisch aus Sicht des Datenschutzes sind besonders auch der Verkauf nicht mehr benötigter Kopierer, die Rückgabe gemieteter Geräte oder deren Entsorgung. Dabei ist in der Regel nicht ausreichend sichergestellt, dass die noch auf den Datenträgern des Kopierers verbliebenen Daten nicht in unbefugte Hände gelangen.

Für den Einsatz der modernen Multifunktionsgeräte sollten einige Regelungen aufgestellt und eingehalten werden, um eine datenschutzkonforme Nutzung der Kopierer zu realisieren. So sollte die Nutzung der Geräte nur berechtigten Personen

möglich sein, was beispielsweise durch den Standort des Kopierers oder durch geeignete Systeme zur Zugangskontrolle, wie Kopierkarten, realisiert werden kann. Weiterhin sind die Standardpasswörter, mit denen die Geräte ausgeliefert werden, bei Inbetriebnahme der Kopierer in geeigneter Weise abzuändern. Originale, Kopien und Ausdrucke sollten immer sofort nach Ende des Druckens oder Kopierens aus dem Gerät entfernt werden. Fehlkopien sollten umgehend datenschutzgerecht, etwa mit einem neben dem Kopierer befindlichen Schredder, vernichtet werden.

Werden die Kopierer als Arbeitsgruppendrucker für mehrere Personen genutzt, so sollten dort möglichst keine Dokumente mit personenbezogenen Daten ausgedruckt werden. Lässt sich dies nicht vermeiden, so sollten die Ausdrucke sofort nach Beendigung des Druckvorgangs aus dem Gerät entfernt werden. Ideal ist es, wenn die Ausdrucke „gesperrt“ werden können: Der Druck wird so lange nicht ausgeführt, bis der zugehörige Auftraggeber direkt am Gerät einen mehrstelligen Code eingibt. So wird sichergestellt, dass die ausgedruckten Dokumente sofort nach Abschluss des Druckvorgangs entfernt werden und dass keine unbefugten Personen Kenntnis der ausgedruckten Daten erhalten können.

Kopiersysteme stellen, wenn sie mit einem Computernetzwerk verbunden sind, eine Vielzahl von Netzdiensten zur Verfügung. Ab Werk werden die Geräte in der Regel so konfiguriert, dass sie möglichst problemlos in Betrieb genommen werden können. So wird sichergestellt, dass zum Beispiel über unterschiedlichste Netzwerkprotokolle mit dem Kopierer kommuniziert werden kann und dass auch von verschiedensten Computersystemen aus auf dem Kopierer gedruckt werden kann. Die Dienste, die für den konkreten Einsatzzweck nicht benötigt werden, sind bei der Inbetriebnahme abzuschalten. Ebenso sind Sicherheitsupdates, die von den Herstellern zur Verfügung gestellt werden, umgehend zu installieren, um bekannte Sicherheitslücken im Kopiersystem zu schließen, gerade dann, wenn die Kopierer innerhalb eines Computernetzwerks betrieben werden.

Wird das Fotokopiersystem in Bereichen eingesetzt, in denen mit sensiblen personenbezogenen Daten gearbeitet wird (zum Beispiel Arztpraxis), soll das Speichern der Daten auf dem Kopiersystem möglichst verschlüsselt erfolgen. Die Daten sind dann gegen missbräuchliche Nutzung geschützt, auch wenn das Kopiergerät beispielsweise gestohlen oder verkauft wird. Wichtig dabei ist, dass die verwendeten Zugangscodes und Passwörter bei Übergabe niemandem mitgeteilt werden. Die verschlüsselte Ablage der Daten auf den Speichermedien kann in der Regel nur durch den Einsatz von „Security-Kits“ realisiert werden. Bei der Neuanschaffung von Kopiergeräten muss ebenfalls berücksichtigt werden, dass das gewünschte Kopiersystem so konfiguriert werden kann, dass die Daten unumkehrbar automatisch gelöscht werden, sobald sie nicht mehr benötigt werden, eine Funktion, die meistens nur über (optional erhältliche) Zusatzmodule mit Namen wie „Security-Kit“ oder „Daten-Sicherheits-Kit (DSK)“ ermöglicht wird. Beim Erwerb eines Kopierers sollte der Hersteller gefragt werden, ob es jederzeit möglich ist, die vollständige Löschung aller Daten manuell anzustoßen, zum Beispiel, wenn das Gerät verkauft oder entsorgt werden soll. Weitere Hintergrundinformationen zur datenschutzgerechten Löschung von Datenträgern sind auf meiner Internetpräsenz unter dem folgenden Link zu finden: http://www.datenschutz-bremen.de/pdf/oh_sicheres_loeschen.pdf.

6.3 Netzsicherheitskonzept für das Migrationsprojekt bremischer Verfahren nach Dataport

Im Berichtsjahr wurde mit der Erstellung eines Konzeptes begonnen, das die Netzinfrastruktur der sog. Bremer Blase, in der die Bremer Verfahren betrieben werden, beschreibt. Im vergangenen Jahr hatte ich über die Migration Bremer Verfahren zu Dataport berichtet und ein Sicherheitskonzept gefordert (vgl. 30. JB, Ziff. 6.1). Das Folgeprojekt mit dem Ziel, die in der Bremer Blase betriebenen Verfahren in die Standard-Rechenzentrums-Netzinfrastruktur am Dataport-Standort in Hamburg zu integrieren, ist ebenfalls berücksichtigt.

Die von mir im Rahmen eines Qualitätszirkels formulierten grundlegenden Anforderungen zur Erhöhung der Sicherheit wurden in das von Dataport erstellte Konzept aufgenommen. Es sind darin aktuelle Konfigurationen beschrieben und zu festgestellten Problembereichen Lösungsansätze festgelegt. Hierzu gehören beispielsweise die Absicherung der Transferverbindungen von Bremen nach Hamburg und damit auch der Zugriff auf Bremer Verfahren und die Einrichtung einer Admin-

Area, mit deren Implementierung der Schutz des administrativen Zugangs zu den Verfahren bereitgestellt bzw. erhöht werden soll. Aussagen zu einem Verfahren zur Protokollierung und Revision fehlen noch.

Der Beginn der Konzeptionierung einer Sicherheitsarchitektur auf Netzebene ist ein sinnvoller Anfang, weil Maßnahmen im Netzbereich oft einen großen Einfluss auf die gesamte IT-Sicherheit haben. Es ist geplant, das vorgelegte Konzept als Grundlage für ein Netzsicherheitskonzept aller Bremer Verfahren in Hamburg zu nehmen und dieses dann in ein allgemeines IT-Sicherheitskonzept für Dataport zu integrieren. Erst dann wird es möglich sein, die vorgeschriebenen Kontrollpflichten des Landes Bremen gegenüber Dataport wahrzunehmen.

6.4 Administrativer Zugang am Dataport-Standort Bremen

Die Senatorin für Finanzen leitete mir Mitte diesen Jahres Unterlagen der Anstalt des öffentlichen Rechts Dataport zu und teilte mir mit, dass geplant sei, über einen einheitlichen und revisionssicheren Weg Administrationstätigkeiten von eine sogenannte Admin-Area in Bremen vorzunehmen. Dadurch soll ein Zugriff von allen Dataport-Arbeitsplätzen an allen Standorten auf Bremer Server und Verfahren ermöglicht werden, die von Dataport betreut bzw. betrieben werden. Beispiele für Administrationstätigkeiten sind unter anderem das Einspielen neuer Programmversionen, die Änderung von Konfigurationseinstellungen sowie die Fehlersuche und -behebung.

Die dafür zur Verfügung gestellten Informationen stammten größtenteils aus einem anderen Dataport-internen Projekt, welches aber bisher nicht umgesetzt worden ist. Auf diese noch nicht abgeschlossen Unterlagen, die auf weitere Dokumente referenzieren, setze ein gesondertes Papier auf, das die Variante für den Dataport-Standort Bremen beschreibt.

Die Unterlagen wurden von mir grob gesichtet und in einem Gespräch mit der Senatorin für Finanzen und Dataport wurde vereinbart, dass zunächst eine für Bremen gültige festgeschriebene Version dieses Konzeptes erstellt wird und noch offene Fragestellungen – beispielsweise zur Revisionssicherheit – geklärt werden. Eine datenschutzrechtliche Bewertung durch mich ist nur auf einer konsolidierten Basis möglich. Ich werde daher erst nach Eingang dieser Unterlagen zu diesem Vorhaben Stellung nehmen.

6.5 Active Directory – Modernisierung des E-Mail-Systems der bremischen Verwaltung

Am 20. Mai 2008 hat der Senat die Modernisierung des E-Mail-Systems der bremischen Verwaltung beschlossen. Das bisher dezentral organisierte System in den Dienststellen soll zukünftig durch eine weitgehende Zusammenfassung von Postfächern bei der BREKOM zentralisiert werden. Das neue System soll auf „Exchange 2007“ laufen, d. h., es muss eine Migration auf das neue System erfolgen. Für die Migrationsphase muss außerdem gewährleistet sein, dass beide Systeme parallel laufen können.

Sowohl die Migrationssphase als auch der zukünftige zentrale Betrieb des E-Mail-Systems werfen eine Reihe von datenschutzrechtlichen Fragen und Problemen auf:

Für die Migrationsphase ist ein funktionierender Verzeichnisdienst erforderlich, das bedeutet den Beginn des Echtbetriebs des Active Directory. Die mit dieser Umstrukturierung des BVN (Bremer Verwaltungsnetz) verbundenen datenschutzrechtlichen Probleme sind bisher nicht gelöst.

Die Durchführung der Migration und der Parallelbetrieb beider Systeme erfordern den Einsatz der Software eines Drittherstellers. Diese soll automatisiert die Analyse der bisherigen Struktur als Vorbereitung der Migration durchführen, beide Systeme für den Parallelbetrieb verbinden und die Verlagerung der Postfächer zur BREKOM unterstützen. Besonders die Analysephase enthält datenschutzrechtlich problematische Prozesse:

— Es besteht ein unbeschränkter Zugriff der BREKOM auf die Exchange-Server der Dienststellen.

— Das Migrationstool bietet umfassende Auswertungsmöglichkeiten, mit denen sich typische Verhaltensweisen von Benutzern analysieren lassen.

Ich habe gegenüber der Senatorin für Finanzen deshalb zunächst grundlegende datenschutzrechtliche Anforderungen formuliert:

— Einsatz einer Auditing-Lösung und Erstellung eines Revisionskonzeptes, die sicherheitsrelevante Prozesse innerhalb des AD (Active Directory) und des E-Mail-Systems transparent und prüfbar machen,

— Einschränkung des Analysetools durch entsprechende Definitionen der Berichtsfilter, die eine Erhebung individueller Kommunikationsdaten verhindern,

— Erstellung eines Sicherheitskonzeptes für die Migration.

Da für die Einführung der neuen E-Mail-Struktur ein erheblicher Zeitdruck festgestellt wurde, ist bereits jetzt abzusehen, dass die komplexen datenschutzrechtlichen Anforderungen vor Beginn der Analysephase nicht vollständig bearbeitet werden können. Ich werde deshalb weiterhin den Prozess intensiv begleiten und habe in Übereinstimmung mit der Senatorin für Finanzen als Auftraggeberin den Abbruch der Analysephase vereinbart, wenn sich erhebliche datenschutzrechtliche Probleme ergeben.

6.6 Virtuelle Poststelle – rechtsverbindliche elektronische Kommunikation mit der bremischen Verwaltung

Im letzten Quartal des Berichtsjahres ist die rechtsverbindliche und vertrauliche Kommunikation mit allen Teilen der bremischen Verwaltung (Eröffnung des elektronischen Rechtsverkehrs) eingeführt worden. Bisher standen lediglich das elektronische Gerichts- und Verwaltungspostfach (EGVP) und das Postfach für das elektronische Meldewesen (Xmeld) zur Verfügung. Mit der Einführung einer allgemeinen virtuellen Poststelle (VPS-Allgemein) kann jeder Bürger und jede Bürgerin mit der Verwaltung elektronisch rechtsverbindlich kommunizieren.

Aufgrund der allgemeinen Einführung dieser Technologie habe ich meine Forderungen nach einem Sicherheitskonzept für die Infrastruktur der virtuellen Poststelle Bremen (Schutzobjekte: Dateien und Systeme zum Betrieb der virtuellen Poststelle) und Datensicherungsmaßnahmen in der virtuellen Poststelle Bremen (Schutzobjekte: Kommunikationsdaten sowie die Dienste (Authentifizierung, Vertraulichkeit, Integrität, Verbindlichkeit, Monitoring/Auditing) gegenüber der Senatorin für Finanzen neu formuliert (vgl. 27. JB, Ziff. 3.1).

Die Senatorin für Finanzen hat daraufhin ein Sicherheitskonzept für die virtuellen Poststellen der Freien Hansestadt Bremen vorgelegt, das sich allerdings als Bindeglied zwischen dem für die Kern- und Webkomponenten der virtuellen Poststelle des Bundes erstellten allgemeinen „Generischen Sicherheitskonzept“ und dem BREKOM-spezifischen Sicherheitskonzept versteht. Da das Dokument zu einem wesentlichen Teil auf die genannten Dokumente verweist und zu konkreten Sicherheitsfragen wenig eigene Informationen liefert, lässt es wesentliche datenschutzrechtliche Fragen unbeantwortet.

Ich habe die Senatorin für Finanzen deshalb aufgefordert, die entsprechenden Sicherheitskonzepte der BREKOM dahingehend zu überprüfen, ob und welche für die virtuellen Poststellen des Landes Bremen erforderlichen Sicherheitseinstellungen dokumentiert sind; ggf. ist eine Ergänzung und Überprüfung erforderlich. Der Bereich der Protokollierung und Revision fehlt und ist deshalb noch zu beschreiben.

6.7 Fernwartung

In der öffentlichen Verwaltung steigt, ebenso wie in der Privatwirtschaft, der Bedarf nach Fernwartung, Remote-Administration und einem funktionierenden User-Helpdesk stetig. Fernwartung macht es möglich, Zeit einzusparen, qualifiziertes Personal und zentrale Ressourcen entsprechend punktgenau einzusetzen. Mitarbeiterinnen und Mitarbeitern kann vom User-Helpdesk zeitnah Unterstützung im Problemfall angeboten werden, notwendige Konfigurationsänderungen bzw. Einstellungen an einer Vielzahl von Arbeitsplatz-Computern können auf ein zeitliches Minimum reduziert und neue Softwareversionen auf Servern von Herstellerfirmen aus der Ferne eingespielt werden, ohne Verzögerungen und Reisekosten. Aus der Sicht des Datenschutzes sind allerdings Rahmenbedingungen einzuhalten. Dazu sind zwei Arten von Fernwartung zu unterschieden:

— Fernwartung für eigene Zwecke ist die interne Anwendung von Fernwartung in großen und/oder verteilten Organisationen, z. B. Verwaltung, Universitätscampus, weitläufige Werksgelände mit mehreren Gebäuden,

— Fernwartung durch Dritte ist die Fernwartung durch externe Organisationen, z. B. Softwarewartung durch Herstellerfirma, Outsourcing des User-Helpdesk.

Die Fernwartung für eigene Zwecke ist aus datenschutzrechtlicher Sicht unter den Vorgaben des § 7 Bremisches Datenschutzgesetz (BremDSG) bzw. § 9 Bundesdatenschutzgesetz (BDSG) nebst der Anlage zu § 9 Satz 1 BDSG zu betrachten.

Fernwartung ist, sofern sie von Dritten durchgeführt wird, rechtlich als Datenverarbeitung im Auftrag gemäß § 9 des Bremischen Datenschutzgesetzes (BremDSG) bzw. § 11 Bundesdatenschutzgesetz (BDSG) einzuordnen. Bei Zweifeln über die Zulässigkeit von Fernwartung, z. B. bei Notaren, Ärzten oder Rechtsanwälten, sollte die zuständige Aufsichtsbehörde zu Rate gezogen werden.

Die Anforderungen des § 7 BremDSG bzw. § 9 BDSG nebst der Anlage zu § 9 Satz 1 BDSG hinsichtlich der technisch-organisatorischen Maßnahmen des Datenschutzes sind auch einer Fernwartung zugrunde zu legen.

Fernwartung sollte nur im Einzelfall und mit Einverständnis (aktive Zustimmung des Betroffenen durch Bestätigung per Mausklick zu Beginn der Fernwartung) des betroffenen Mitarbeiters durchgeführt werden. Fernwartung ohne unmittelbare Einwilligung darf nicht möglich sein. Die Aktivitäten während der Fernwartung sollten immer vom Betroffenen kontrolliert werden, idealerweise durch Beobachtung der Aktivitäten auf dem lokalen Bildschirm.

Der komplette Akt der Fernwartung sollte protokolliert werden, um eine spätere Revision zu ermöglichen. Die maximale Aufbewahrungsdauer dieser Protokolle ist festzulegen.

Der Kreis derer, die überhaupt Fernwartungen durchführen dürfen, ist eng zu begrenzen ebenso wie die Zugriffsmöglichkeiten im Rahmen der Fernwartung auf das erforderliche Maß zu beschränken sind. Ein Administrator einer Fachanwendung benötigt in der Regel keine Systemverwalterprivilegien für die gesamte EDV.

Neue Softwareversionen sollten grundsätzlich nicht im Rahmen der Fernwartung installiert werden. Hier gibt es geeignetere Methoden, wie z. B. das Mittel der Softwareverteilung.

Wird die Fernwartung durch Dritte durchgeführt, so sollten Art und Umfang der Wartungsarbeiten differenziert vertraglich geregelt werden. Gleiches gilt für die Verpflichtung des Auftragnehmers, die für den Auftraggeber geltenden datenschutzrechtlichen Bestimmungen einzuhalten, und auch die Untersagung, dass personenbezogene Daten, die im Rahmen der Datenverarbeitung offenbart werden, weitergegeben werden.

Bereits im letzten Jahr habe ich den Einsatz eines Fernwartungstools bei Dataport begleitet (vgl. 30. JB, Ziff. 6.2). In diesem Zusammenhang habe ich klare Regelungen für den Einsatz von Fernwartungstools gefordert. Da sich bei mir die Anfragen zur Ausgestaltung von Fernwartung häufen, rege ich dringend an, dass eine für die bremische Verwaltung allgemein gültige Richtlinie „Fernwartung“ erstellt wird, die die oben genannten Punkte berücksichtigt.

6.8 Bericht aus dem Arbeitskreis Grundsatzfragen der Verwaltungsmodernisierung

Der Arbeitskreis der Datenschutzbeauftragten des Bundes und der Länder thematisierte: EU-Dienstleistungsrichtlinie, Binnenmarktinformationssystem (kurz: IMI für Internal Market Information System), ePayment und Ratsinformationssysteme. Daneben spielten die Geodatenverarbeitung im Hinblick auf den Entwurf des Geodatenzugangsgesetzes und die Auftragsdatenverarbeitung insbesondere im Bereich der Übertragung von kommunaler Inkassotätigkeit und im Bereich von Berufsgeheimnisträgern eine bedeutende Rolle.

Die EU-Dienstleistungsrichtlinie als Bestandteil der Lissabonner Ziele der EU verfolgt strategisch die Schaffung von Arbeitsplätzen, Wirtschaftswachstum und mehr grenzüberschreitenden Handel mit Dienstleistungen. Zur Erreichung dieser Ziele sollen Verwaltungsverfahren effektiver gestaltet, Genehmigungsverfahren gestrafft und bürokratische Hindernisse bei der Aufnahme von Dienstleistungstätigkeiten

abgebaut werden. Die Umsetzung der EU-Dienstleistungsrichtlinie stellt neue Anforderungen an die Vernetzung der Prozess- und IT-Strukturen der öffentlichen Verwaltung und sieht u. a. einheitliche Ansprechpartner, elektronische Verfahrensabwicklung und Genehmigungsfiktion bei Fristüberschreitung vor. Der Datensicherheit ist hier viel Bedeutung beizumessen.

6.9 Bericht aus dem Arbeitskreis Technik

Eine regelmäßige Beteiligung am Arbeitskreis (AK Technik) der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist unerlässlich. Zentrale Themen des Arbeitskreises im Berichtsjahr waren u. a.

— das Antragsverfahren für die neuen ePässe; in verschiedenen Bundesländern wurden bei Prüfungen technische Mängel festgestellt. Der AK Technik hielt im Sommer zusammen mit dem Bundesministerium des Innern (BMI) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Workshop ab, bei dem BMI und BSI den aktuellen Umsetzungsstand der Einführung der ePässe darlegten und die von den Datenschutzbeauftragten festgestellten Mängel präsentiert und diskutiert wurden,

— das Projekt oscare, eine IT-Lösung für gesetzliche Krankenversicherungen (GKV), die sämtliche Geschäftsprozesse einer GKV abbildet. Kernfragen dabei sind insbesondere das notwendige Berechtigungskonzept, das den Zugriff auf die Versichertendaten regelt und die Protokollierung schreibender und lesender Zugriffe auf die Daten der Krankenkassen,

— die Auswirkungen des Urteils des Bundesverfassungsgerichts vom 27. Februar 2008 zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und

— technische Verfahren zur Kennzeichnung der Herkunft von Daten, wie sie sich in der aktuellen Diskussion um die Novellierung des Bundesdatenschutzgesetzes (BDSG) im Zuge der jüngsten Datenskandale um den Adresshandel ergeben.

7. Bremische Bürgerschaft

7.1 Ergebnisse der Beratungen des 30. Jahresberichts

B e r i c h t und A n t r a g des Ausschusses für Informations- und Kommunikationstechnologie und Medienangelegenheiten zum 30. Jahresbericht des Landesbeauftragten für Datenschutz vom 31. März 2008 (Drs. 17/325) und zur Stellungnahme des Senats vom 19. August 2008 (Drs. 17/509)

I. Bericht

Die Bürgerschaft (Landtag) überwies in ihrer Sitzung am 7. Mai 2008 den 30. Jahresbericht des Landesbeauftragten für den Datenschutz vom 31. März 2008 (Drucksache 17/325) und in ihrer Sitzung am 10. September 2008 die dazu erfolgte Stellungnahme des Senats vom 19. August 2008 (Drucksache 17/509) an den Ausschuss für Informations- und Kommunikationstechnologie und Medienangelegenheiten zur Beratung und Berichterstattung.

Der Ausschuss stellte im Rahmen der Behandlung des 30. Jahresberichts und der Stellungsnahme des Senats bei den nachfolgend aufgeführten Punkten Beratungs- und Handlungsbedarf fest:

1. Ziffer 6.3 Zentrale Protokollierung der Internetnutzung der bremischen Verwaltung,
2. Ziffer 7.1 Ergebnisse der Beratung des 29. Jahresberichts,
3. Ziffer 9.16 Verfahren ADVIS und BONITAET beim Stadtamt Bremen,
4. Ziffer 9.17 Übermittlung von Meldedaten an politische Parteien vor den Wahlen,
5. Ziffer 12.3.1 Kindeswohlgesetz.

In seiner Sitzung am 10. Oktober 2008 erörterte der Ausschuss die beratungsbedürftigen Punkte mit dem Landesbeauftragten für den Datenschutz unter Hinzuziehung der Vertreter der betroffenen Ressorts.

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

1. Zentrale Protokollierung der Internetnutzung der bremischen Verwaltung (Ziff. 6.3): Im Rahmen einer Datenschutzprüfung der Protokollierung dienstlicher und privater Internetaktivitäten der bremischen Verwaltung bei der BREKOM stellte der Landesbeauftragte für den Datenschutz fest, dass bei Logs und Protokollen auf dem Server für die private Nutzung die vollständigen IP-Adressen der Rechner innerhalb des BVN protokolliert wurden, von denen die jeweiligen Anfragen stammten. Dies steht im Widerspruch zu der im Amtsblatt 2004-20 der Freien Hansestadt Bremen veröffentlichten „Richtlinie für die Bereitstellung und Nutzung von Internet/Intranetzugängen“ und verstößt gegen das Telemediengesetz. Die unzulässigen Dateien waren zum Zeitpunkt der Überprüfung bis zu drei Wochen alt. Dem Landesbeauftragten für den Datenschutz wurde von der BREKOM berichtet, dass drei Wochen vor der Überprüfung der Proxy-Server für die private Internetnutzung neu installiert werden musste und dabei versehentlich sowohl das Regelwerk für die dienstliche Nutzung eingestellt als auch die Rotation nicht entsprechend angepasst und kontrolliert worden sei. Daraufhin rotierten die Mitarbeiter der BREKOM die fehlerhaften Log- und Protokolldateien und reduzierten die IP-Adresse auf die Netzadresse der Anfrage. Der Landesbeauftragte für Datenschutz verlangte in seinem Prüfbericht, dass die Entstehung des Fehlers genau untersucht und ihm nachgewiesen wird, wie zukünftig derartige Fehlkonfigurationen vermieden werden können.

Die Senatorin für Finanzen erläuterte, dass mit der BREKOM organisatorische Maßnahmen verabredet worden seien, um in Zukunft derartige Fehler zu vermeiden. Die Protokollierung der dienstlichen und privaten Internetaktivitäten habe streng getrennt voneinander zu erfolgen, um so zu verhindern, dass das falsche Regelwerk eingestellt werde. Zudem solle nach dem Vier-Augen-Prinzip verfahren werden, wonach die von einem Mitarbeiter vorgenommenen Einstellungen von einem zweiten auf ihre Richtigkeit überprüft und abgezeichnet werden.

Der Ausschuss nimmt die getroffenen Maßnahmen zur Kenntnis und geht davon aus, dass die aufgetretenen Fehler dadurch in Zukunft verhindert werden können, sodass dieser Punkt als erledigt angesehen werden kann.

2. Verschriftungssoftware bei der TK-Überwachung (Ziffer 7.1): Hinsichtlich der Telekommunikationsüberwachung der Polizei war bereits dem Rechtsausschuss im Rahmen der Beratungen zum 28. Jahresbericht und dem Ausschuss für Informations- und Kommunikationstechnologie und Medienangelegenheiten bei den Beratungen zum 29. Jahresbericht vom Landesbeauftragten für den Datenschutz mitgeteilt worden, dass die Prüfung der Telekommunikationssoftware der Polizei technische und organisatorische Mängel offenbarte. Einige Mängel sind behoben worden, weiterhin problematisch bleibt aber die fehlende Zugriffs- und Eingabekontrolle bei der Verschriftungssoftware TÜPFO. Der Senator für Inneres und Sport legte dem Ausschuss im Rahmen der Beratungen zum 29. Jahresbericht dar, dass die Software ohne Abstriche für ihre Einsatzfähigkeit nicht umgestaltungsfähig sei und kündigte die Umstellung auf eine neue Software an, die Mitte des Jahres 2009 betriebsfähig sein werde. Der Landesbeauftragte für den Datenschutz berichtete, dass in der Zwischenzeit eine akzeptable Übergangslösung bis zur Umstellung auf die neue Software geschaffen worden sei, bei der die Protokollierung, wie gefordert, zentral erfolge. Der Ausschuss erwartet die Einführung der neuen Software bis spätestens Ende des Jahres 2009 und betrachtet diesen Punkt im Übrigen als erledigt.

3. Rahmendatenschutzkonzept Stadtamt (Ziffer 7.1): Bereits im Jahr 2006 hatte sich der Rechtsausschuss mehrfach mit den seit mehreren Jahren beim Stadtamt Bremen zu verschiedenen DV-Verfahren ausstehenden Fachdatenschutzkonzepten und dem fehlenden Rahmendatenschutzkonzept beschäftigt und dazu der Bremischen Bürgerschaft zum 28. Jahresbericht berichtet.

Im Januar 2007 wurde der Entwurf eines Rahmendatenschutzkonzeptes vorgelegt, die verbliebenen Kritikpunkte wurden im April 2007 im Rechtsausschuss behandelt. Bis September 2008 sollte ein neues Rahmendatenschutzkonzept des Stadtamtes in Abstimmung mit dem Landesbeauftragten für den Datenschutz erstellt werden. Der Senator für Inneres und Sport erläuterte, dass aufgrund zurzeit noch fehlender Anlagen mit einer Fertigstellung des Rahmendatenschutzkonzeptes erst bis Mitte November 2008 zu rechnen sei. Der Landesbeauftragte für den Datenschutz erklärte, dass er danach baldmöglich eine abschließende Stellungnahme gegenüber

dem Stadtamt abgeben werde, die Einarbeitung seiner Vorschläge könne daher voraussichtlich erst im Januar 2009 erfolgen.

Darüber hinaus stehen noch diverse Fachdatenschutzkonzepte, in denen Sicherheitsmaßnahmen zu konkreten Verfahren beschrieben werden, zur abschließenden Bearbeitung aus.

Der Landesbeauftragte für den Datenschutz teilte dem Ausschuss in seiner Sitzung am 10. Oktober 2008 mit, dass er im April um eine Zurückstellung der Fachdatenschutzkonzepte gebeten worden sei, um eine Fertigstellung des Rahmendatenschutzkonzeptes noch in diesem Jahr zu ermöglichen. Dem habe er zugestimmt.

Der Ausschuss bittet den Senator für Inneres und Sport und den Landesbeauftragten für den Datenschutz darum, ihn über die Umsetzung des Rahmendatenschutzkonzepts in die Praxis Ende Februar 2009 zu unterrichten. Der Ausschuss sieht mit dieser Berichterstattung den Punkt als erledigt an.

4. Verfahren ADVIS und BONITAET beim Stadtamt (Ziffer 9.16): In der Verfahrensbeschreibung und in dem Datenschutzkonzept des Verfahrens BONITAET waren die Rechtsgrundlagen nicht zutreffend aufgeführt. Zudem erfolgte die Darstellung der verarbeiteten Datenkategorie teilweise zu allgemein oder unzutreffend. Es konnte nicht nachvollzogen werden, wer Eingaben oder Zugriffe in dem Programm tätigte, da aus technischer Sicht eine Authentifizierung und Protokollierung fehlte. Zwar teilte das Stadtamt dem Landesbeauftragten für den Datenschutz im November 2007 verschiedene Änderungen mit, es blieb aber offen, wie viele Personen auf das Programm zugreifen, ob eine Anmeldung an dem Verfahren und eine Protokollierung der Benutzeraktivitäten erfolgt. Eine ergänzende Antwort darauf blieb bisher aus.

Im Rahmen des Verfahrens ADVIS fehlte eine klare Trennung der Datenverarbeitung nach dem Aufenthaltsgesetz sowie der Aufenthaltsverordnung einerseits und dem Ausländerzentralregistergesetz und seiner Durchführungsverordnung andererseits. Bei der Angabe der Rechtsgrundlagen, der Beschreibung der Datenkategorien und der Verwendungszwecke bestanden Unklarheiten und Unrichtigkeiten. Zudem ergaben sich verschiedene Fragen zur Datensicherheit des Verfahrens.

Der Landesbeauftragte für den Datenschutz teilte dem Ausschuss in seiner Sitzung am 10. Oktober 2008 mit, dass die Verfahrensbeschreibung für das Verfahren ADVIS zurückgestellt worden sei, um eine schnellere Bearbeitung des Rahmendatenschutzkonzeptes zu ermöglichen. Bezüglich des Verfahrens BONITAET ging zwischenzeitlich ein Schreiben vom Senator für Inneres beim Landesbeauftragten für den Datenschutz ein, wonach das Verfahren zwischenzeitlich eingestellt worden sei.

Der Ausschuss nimmt die Ausführungen des Landesbeauftragten für den Datenschutz zur Kenntnis und schließt den Punkt damit ab.

5. Übermittlung von Meldedaten an politische Parteien vor den Wahlen (Ziffer 9.17 dieses Berichts): Im Vorfeld der Wahlen zur Bremischen Bürgerschaft und zur Stadtverordnetenversammlung Bremerhaven wurden von den Meldebehörden in Bremen und Bremerhaven Daten von wahlberechtigten Einwohnern an Parteien weitergegeben, die an den Wahlen teilnahmen. In Bremerhaven erfolgte die öffentliche Bekanntmachung des Widerspruchsrechts erst verspätet. Der Landesbeauftragte für den Datenschutz forderte die Meldebehörde Bremerhaven auf, bei künftigen Wahlen das Widerspruchsrecht rechtzeitig bekannt zu geben. Der Senator für Inneres und Sport teilte dem Ausschuss in seiner Sitzung am 10. Oktober 2008 mit, dass nach einer gesetzlichen Änderung die öffentliche Bekanntmachung nach § 33 Abs. 1 Satz 7 BremMeldG nun nicht mehr „rechtzeitig“, sondern innerhalb einer „Frist von acht Monaten“ erfolgen müsse. Damit sei die Frage, wann die Bekanntmachung „rechtzeitig“ erfolge, geklärt. Die Meldebehörden seien verpflichtet, sich an die nun festgelegte gesetzliche Frist zu halten.

Der Ausschuss nimmt die Ausführungen des Senators für Inneres und Sport zur Kenntnis und schließt den Punkt damit ab.

6. Kindeswohlgesetz (Ziffer 12.3.1): Das Gesetz zur Sicherung des Kindeswohls und zum Schutz von Kindesvernachlässigung (KIWG) trat am 1. Mai 2007 in Kraft. Mit dem elektronischen Verfahren „Einladungswesen“ wurde am 1. Dezember 2007 begonnen, obwohl noch kein fachspezifisches Datenschutzkonzept erstellt worden war. Ende November 2007 wurde dem Landesbeauftragten für den Datenschutz

eine Verfahrensbeschreibung übersandt, allerdings steht die von Gesetzes wegen notwendige Festlegung der technisch-organisatorischen Maßnahmen noch aus. Die Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales führte in der Ausschusssitzung am 10. Oktober 2008 aus, dass zurzeit mit einer technischen Übergangslösung gearbeitet werde, die notwendig gewesen sei, um rechtzeitig mit dem Einladungswesen zu beginnen. Aus diesem Grund sei das Datenschutzkonzept noch nicht fertiggestellt worden. Zu Beginn des kommenden Jahres werde die neue Software in Betrieb genommen. Bis dahin solle das fachspezifische Datenschutzkonzept in Abstimmung mit dem Landesbeauftragten für den Datenschutz vollständig erstellt sein.

Der Ausschuss nimmt die Ausführungen zur Kenntnis und bittet den Landesbeauftragten für den Datenschutz um einen weiteren Bericht, sofern es bei der Abstimmung des Datenschutzkonzeptes zu Problemen kommt. Ansonsten sieht der Ausschuss den Punkt als erledigt an.

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 vorgenannte Behandlung des 30. Jahresberichts zum Datenschutz und der Stellungnahme des Senats konnte nach eingehender Beratung im Ausschuss für Informations- und Kommunikationstechnologie und Medienangelegenheiten der Bremischen Bürgerschaft (kurz Medienausschuss) erstmalig noch im gleichen Jahr mit einer Debatte in der Bürgerschaft (Landtag) abgeschlossen werden. Durch die Unterstützung des Ausschusses konnten in allen genannten Punkten Verbesserungen für den Datenschutz erreicht werden, dies gilt insbesondere auch für die sog. Restanten aus vorhergehenden Jahresberichten. Der Medienausschuss hat sich darüber hinaus für eine ganze Reihe weiterer aktueller Punkte interessiert, von denen ich hier einige aufführen will.

So ließ sich der Ausschuss über verschiedene Fälle von in der Presse hervorgehobenen Datenschutzverstößen unterrichten. Dabei ging es u. a. um den Vorwurf des Verstoßes gegen die ärztliche Schweigepflicht, Fragen des Adresshandels oder den Einsatz von Videoüberwachungskameras bei dem Discounter Lidl. Die Datenpanne bei Einwohnermeldeämtern im Modul „Onlineabfrage“ führte sogar zu einer Sondersitzung. Selbstverständlich waren auch die verschiedenen, in der Presse unter der Überschrift „Datenklau“ behandelten Fälle Themen in Ausschusssitzungen und führten darüber hinaus mit Anträgen von FDP und CDU „Datenschutzbewusstsein der Bevölkerung stärken“ (Drs. 17/522) und von SPD und Bündnis 90/Die Grünen „Datenmissbrauch bekämpfen – Datenschutzbewusstsein stärken“ (Drs. 17/533) zur Debatte und Beschlussfassung in der Bremischen Bürgerschaft (vgl. Protokoll vom 10.09.2008, S. 1973). Ausführlich beschäftigte sich der Ausschuss mit datenschutzrechtlichen Aspekten eines Strukturwandels durch die Migration verschiedener DV-Systeme zu Dataport. Ebenfalls in diesem Zusammenhang können die Große Anfrage der Fraktionen von Bündnis 90/Die Grünen und der SPD mit dem Thema „Weiterentwicklung des IT-Bereichs der bremischen Verwaltung“ (vgl. Drs. 17/481) und die Stellungnahme des Senats (vgl. Drs. 17/534) gesehen werden, hier sind die Fragen 4. und 6. aus Datenschutzsicht hervorzuheben.

Schließlich waren auch die an den Autobahnen A 1 und A 27 von der Verkehrsmanagementzentrale angebrachten Webcams Thema der Beratungen (Näheres hierzu vgl. Ziff. 14.2). Insgesamt ist es gelungen, mit Hilfe des Ausschusses eine Struktur zu entwickeln, die eine angemessene und effektive Behandlung der jeweils anstehenden Datenschutzthemen ermöglicht.

7.3 Abschaffung der automatischen Kfz-Kennzeichenerfassung

Das Bundesverfassungsgericht (BVerfG) hat am 11. März 2008 (Az. 1 BvR 2074/05 und 1 BvR 1254/07) entschieden, dass die automatisierte Erfassung amtlicher Kennzeichen von Kraftfahrzeugen, das sogenannte Kennzeichenscreening, unzulässig ist. Gegenstand der Entscheidung waren Verfassungsbeschwerden gegen polizeirechtliche Vorschriften in Hessen und Schleswig-Holstein. Das Gericht hat festgestellt, dass die angegriffenen Vorschriften das Grundrecht auf informationelle Selbst-

bestimmung verletzen. Insbesondere genügten die Vorschriften zum Kennzeichenscreening nicht den verfassungsrechtlichen Geboten der Normenklarheit sowie dem Verhältnismäßigkeitsprinzip.

Das Bremische Polizeigesetz (BremPolG) enthielt mit § 29 Abs. 6 BremPolG eine vergleichbare Befugnisnorm. Die Bürgerschaft hat sofort reagiert und unmittelbar nach der Entscheidung des BVerfG im Sommer dieses Jahres diese Norm im BremPolG abgeschafft. In der Debatte wurde dabei hervorgehoben, dass die Regelung in Bremen ohnehin ins Leere gelaufen sei, weil es keinen Einsatz entsprechender Technik in Bremen und Bremerhaven gegeben habe.

8. Personalwesen

8.1 Verschwinden einer Referendarakte im häuslichen Bereich eines Schulleiters

Auf die Bitte um Einsicht in seine Akte erhielt ein Referendar vom Schulleiter zunächst die Antwort, die Akte befinde sich bei ihm zu Hause. Später erklärte er, sie sei aufgrund eines Wasserschadens nicht mehr vorhanden. Die Akte enthielt u. a. vom Referendar erstellte Unterrichtsunterlagen sowie Beurteilungen. Da durch das Verschwinden der Referendarakte das Akteneinsichtsrecht des Betroffenen vereitelt wurde und Anhaltspunkte vorliegen, dass dadurch schutzwürdige Interessen verletzt sind, fragte ich die Senatorin für Bildung und Wissenschaft, in welcher Weise gewährleistet werden könne, dass ein Verschwinden derartiger Akten zukünftig nicht mehr vorkomme, z. B. durch Rückgabe an die Referendarinnen und Referendare. Die Senatorin für Bildung und Wissenschaft teilte dazu mit, sie habe entschieden, dass zukünftig Materialien von Referendarinnen und Referendaren entweder zur Akte genommen oder ihnen übergeben werden müssen.

8.2 Bericht aus dem Arbeitskreis Personalwesen

Im Berichtszeitraum hat der Arbeitskreis der Datenschutzbeauftragten des Bundes und der Länder einmal getagt und schwerpunktmäßig folgende Themen beraten: Datenerhebung im polizeilichen Bewerberauswahlverfahren, Initiative zur Aufnahme von Vorschriften zum Arbeitnehmerdatenschutz in ein Arbeitsvertragsgesetz, Einsatz der elektronischen Gesundheitskarte im Rahmen der Beihilfebearbeitung, Einzel- und Gruppenzielvereinbarung zur gerechten Bezahlung von Leistungsprämien, Erfahrungsaustausch über das Betriebliche Eingliederungsmanagement, Allgemeines Gleichbehandlungsgesetz, Dienstrechtsneuordnungsgesetz.

8.3 Geschäftsverteilungspläne der Finanzämter im Intranet

Im Intranet der Finanzverwaltung enthielten die Geschäftsverteilungspläne auch Personalaktendaten, die dem Personalaktengeheimnis nach § 93 a Abs. 1 Satz 1 Bremisches Beamtengesetz unterliegen, z. B. Hinweise auf Teilzeitbeschäftigung und Umfang der Arbeitszeit, zugeordnete Mitarbeiterinnen und Mitarbeiter, Elternzeit sowie Altersteilzeiten (aktive Phase und Freistellungsphase).

Aufgrund meiner Anfrage sind die Pläne unverzüglich aus dem Intranet entfernt und nach datenschutzrechtlicher Überprüfung nunmehr ohne die von mir monierten Personaldaten wieder ins Intranet gestellt worden.

9. Inneres

9.1 Unberechtigter Zugriff auf Online-Melderegister war möglich

Wenige Stunden vor Ausstrahlung eines Fernsehberichts über eine Sicherheitslücke einer Internetkomponente einer Einwohnermeldeamtssoftware, die auch im Land Bremen zum Einsatz kommt, wurde ich von Kollegen aus einem anderen Bundesland darüber in Kenntnis gesetzt. Ich setzte mich umgehend mit den Einwohnermeldeämtern in Bremen und Bremerhaven in Verbindung. Für Bremen konnte sofort Entwarnung gegeben werden, da nach Auskunft des Stadtamtes das entsprechende Softwaremodul noch nicht zum Einsatz gekommen war. Anders in Bremerhaven, wo die Online-Melderegisterauskunft bereits im Einsatz war. Beim dortigen Bürger- und Ordnungsamt führte ich umgehend eine Datenschutzprüfung des betroffenen Moduls durch. Sowohl das Amt als auch die b.i.t. (technischer Betreiber) zeigten sich bei der Prüfung sehr kooperativ. Im Rahmen der Prüfung konnte ich feststel-

len, dass die Sicherheitslücke in Bremerhaven tatsächlich bestand: Ein Standardpasswort eines Benutzerkontos, mit dem die Software immer ausgeliefert wird, war nicht in geeigneter Form geändert worden. Protokolldaten gaben Auskunft darüber, dass es seit 2005 Zugriffe aus dem Internet unter der besagten Benutzerkennung gegeben hatte, die aber fast immer eindeutig im Rahmen von Wartungsarbeiten dem Softwarehersteller oder der b.i.t zuzuordnen waren. Allerdings gab es im Mai 2008 einmalig Zugriffe, die nicht Wartungsarbeiten oder, das hat eine Rückfrage beim Fernsehsender ergeben, den Recherchen im Zusammenhang mit dem Fernsehbericht zuzuordnen waren; ich musste daher von einer unberechtigten Nutzung ausgehen. Bei diesen Zugriffen wurden verschiedene Bereiche des Software-Moduls aufgerufen. Aus den Protokolldaten ist jedoch ersichtlich, dass keine Daten Bremerhavener Bürger eingesehen wurden. Eine Benachrichtigung betroffener Bürger durch das Bürger- und Ordnungsamt war somit nicht notwendig.

Die Herstellerfirma handelte grob fahrlässig, indem sie die Software mit einem Standardpasswort ausgeliefert und dieses Standardpasswort auf einer ihrer Web-Seiten versehentlich veröffentlicht hatte. Ich habe das Bürger- und Ordnungsamt aufgefordert, die Mängel abzustellen und erst nach deren Beseitigung die Online-Melderegisterauskunft wieder in Betrieb zu nehmen.

9.2 Übermittlung von Meldedaten an Adresshändler

Bedingt durch die Datenskandale geriet der Adresshandel in das Blickfeld der Öffentlichkeit. In diesem Zusammenhang wurde auch die Rolle der Melderegister von den Medien, so auch von Radio Bremen, ins Visier genommen.

Nach den melderechtlichen Bestimmungen dürfen die Meldebehörden in Bremen und Bremerhaven Auskünfte über im Melderegister gespeicherte Einwohnerinnen und Einwohner auch an Privatpersonen erteilen. Voraussetzung für die Erteilung einer sogenannten einfachen Melderegisterauskunft nach § 32 Abs. 1 des bremischen Meldegesetzes (BremMeldG), bei der die Meldebehörde Auskunft über Vor- und Familiennamen, Doktorgrade und Anschriften erteilt, ist, dass die auskunftsersuchende Person oder Stelle den Betroffenen hinreichend bestimmt. Soweit ein berechtigtes Interesse glaubhaft gemacht wird, dürfen die Meldebehörden gem. § 32 Abs. 2 BremMeldG eine erweiterte Melderegisterauskunft u. a. auch über frühere Vor- und Familiennamen, Tag und Ort der Geburt, Staatsangehörigkeiten, den Familienstand, gesetzliche Vertreterinnen und Vertreter sowie Anschriften von Ehegatten erteilen. Melderegisterauskünfte über eine Vielzahl nicht namentlich bezeichneter Einwohnerinnen und Einwohner mit einem § 32 Abs. 2 BremMeldG vergleichbaren Datenumfang dürfen die Meldebehörden im Rahmen einer sogenannten Gruppenauskunft nach § 32 Abs. 3 BremMeldG an den genannten Empfängerkreis übermitteln. Die Entscheidung über die Erteilung einer Auskunft nach § 32 BremMeldG liegt jeweils im Ermessen der Meldebehörde.

Nicht selten werden von den Meldebehörden in Bremen und Bremerhaven Melderegisterauskünfte nach § 32 BremMeldG auch an Adresshandelsunternehmen übermittelt, die im Auftrag eines Unternehmens oder einer Privatperson als Adressermittler tätig werden. Hintergrund des Auftrags kann z. B. die Geltendmachung einer finanziellen Forderung gegenüber einem Schuldner sein, wenn dessen Anschrift dem Gläubiger nicht bekannt ist. Häufig werden die über den Adressermittlungsauftrag von den Adresshandelsunternehmen bei den Meldebehörden erhobenen Daten über den Auftrag hinaus in eigenen Datenbanken fortgespeichert, um danach Auskünfte hieraus oder durch den listenmäßigen Verkauf von Daten weitere Einnahmen erzielen zu können. Auf diesem Wege entstehen im privaten Bereich weitere partielle Einwohnermelderegister. Dies stellt eine Zweckänderung dar und ist mit den datenschutzrechtlichen Anforderungen an den Adresserhebungsauftrag und den Vorgaben des Melderechts nicht zu vereinbaren. Die Melderegister dienen vorrangig der staatlichen Aufgabenerfüllung. Sie bieten daneben nicht öffentlichen Stellen und Privatpersonen auf der Grundlage der gesetzlichen Bestimmungen auch Unterstützung an. Da die Bürgerinnen und Bürger zur Abgabe der in den Melderegistern zu speichernden Daten verpflichtet sind, bedürfen sie eines weitergehenden Schutzes. Die Führung von Datenbanken durch Adresshandelsunternehmen mit von ihnen bei den Meldebehörden erhobenen Daten widerspricht den Intentionen des Melderechts. Die nach den melderechtlichen Bestimmungen zu beachtenden schutzwürdigen Interessen der Betroffenen finden bei den Privaten keine Berücksichtigung mehr.

Den Meldebehörden ist daher nahegelegt, im Rahmen ihrer Ermessensentscheidung zumindest keine Meldedaten mehr an die betreffenden Adresshandelsunternehmen herauszugeben, bei denen eine zweckwidrige Verwendung der Meldedaten festgestellt wurde. Darüber hinaus ist die Regelung zur Herausgabe von Meldedaten an Adressbuchverlage ohne Einwilligung der Betroffenen zur Erstellung von Adressbüchern zu überprüfen. Da das Melderecht dem Bund übertragen wurde, sind diese Überlegungen bei der Schaffung eines einheitlichen Bundesmeldegesetzes (vgl. Ziff. 9.4 dieses Berichts) anzustellen.

9.3 Direktzugriff auf Meldedaten durch Behörden

Nach § 30 Abs. 4 Bremisches Meldegesetz (BremMG) erhalten Behörden nur aufgrund einer Rechtsverordnung einen Direktzugriff auf Meldedaten, d. h., diese Stellen können Daten online unmittelbar aus dem Melderegister abrufen. Der Senator für Inneres und Sport hat jedoch Anfang 2007 per Erlass verfügt, dass dieser Vorbehalt einer Rechtsverordnung nicht für Datenabrufe durch Behörden innerhalb einer Gemeinde gilt, der die Meldebehörde angehört. Begründet wird dies damit, § 30 Abs. 5 BremMG enthalte eine entsprechende Ermächtigung. Vielmehr soll nunmehr eine Prüfung ausreichen, ob die angeforderten Daten von der empfangenden Behörde regelmäßig zur Aufgabenerfüllung benötigt werden. Auch sei zu untersuchen, ob und ggf. in welchem Umfang mit der Nutzung des Abrufverfahrens Gefahren für die Rechte der Betroffenen verbunden sind. Der benötigte Datenumfang sei nachprüfbar festzulegen.

Von diesem Erlass habe ich erst im Frühjahr 2008 erfahren. Ich halte den Erlass nicht für rechtskonform und habe der senatorischen Behörde mitgeteilt, die Regelung des § 30 Abs. 5 BremMG besagt ausschließlich, dass derartige Behörden mehr Meldedaten (z. B. Religionszugehörigkeit, Angaben über Ehepartner bzw. Lebenspartner) erhalten können als Behörden, die nicht der Gemeinde der Meldebehörde angehören. Diese Regelung bezieht weder die regelmäßige Datenübermittlung noch den automatisierten Datenabruf ausdrücklich ein. Seit Bestehen des bremischen Meldegesetzes und der technischen Möglichkeit eines automatisierten Abrufs sind viele Regelungen in der Meldedatenübermittlungsverordnung geschaffen worden.

Auch datenschutzpolitisch vermag ich im Übrigen ein Absehen von einer Rechtsverordnung, die die Informationsaustauschwege bei Meldedaten offen legt, nicht nachvollziehen. In weiten Bereichen der Verwaltung sollen die Bürgerinnen und Bürger möglichst umfassend über das Verwaltungshandeln informiert und dadurch Transparenz hergestellt werden. Aber hier, wo eine „Datenautobahn“ eingerichtet werden soll, sollen die betroffenen Bürgerinnen und Bürger nicht einmal erfahren, welche Datenpakete sich darauf bewegen dürfen. Der Wegfall der datenschutzrechtlichen Überprüfung der Zulässigkeit der Datenübermittlung bzw. -weitergabe an eine andere Stelle muss kompensiert werden. Dies geschieht in einer Rechtsverordnung, die für jedermann erkennbar offenlegt, welche Daten aus welchem Anlass zu welchem Zweck an wen übermittelt bzw. weitergegeben werden dürfen.

Der Senator für Inneres und Sport hält die bisherige datenschutzkonforme Praxis nach wie vor unter Hinweis auf die Strukturierung des § 30 BremMG nicht mehr für angezeigt. Er beharrt auf seiner Position, obwohl ich ihn auch nach einer Umfrage unter den Datenschutzbeauftragten des Bundes und der Länder, die meine Rechtsauffassung teilen, aufgefordert habe, den Erlass aufzuheben und an der bisherigen Praxis festzuhalten.

9.4 Entwurf eines Bundesmeldegesetzes

Mit dem Gesetz zur Änderung des Grundgesetzes vom 28. August 2006 (BGBl. I S. 2034) wurde dem Bund gem. Art. 73 Abs. 1 Nr. 3 Grundgesetz die ausschließliche Gesetzgebung für das Melde- und Ausweiswesen übertragen. Hierzu hat der Bundesminister des Innern nun im Berichtsjahr den Referentenentwurf eines Gesetzes zur Fortentwicklung des Meldewesens (Bundesmeldegesetz) vorgelegt. Mit dem Gesetz sollen die Grundlagen für ein einheitliches Melderecht und die Errichtung zentraler Registerstrukturen für einen effektiveren und effizienteren Vollzug des Melderechts geschaffen werden. Der Entwurf aus dem Bundesministerium des Innern entspricht in zahlreichen Punkten nicht den Forderungen des von den Datenschutzbeauftragten des Bundes und der Länder erarbeiteten Eckpunktepapiers. Ich habe den Senator für Inneres und Sport hierüber unterrichtet und ihn um Unterstützung der datenschutzrechtlichen Forderungen gebeten.

Im Einzelnen sieht der Referentenentwurf ein zusätzliches zentrales Bundesmelderegister und damit eine doppelte Datenhaltung vor. Das Vorhaben widerspricht dem Grundsatz der Datenvermeidung, der Vermeidung einer doppelten Datenstruktur und dem Erforderlichkeitsprinzip. Die bisherige dezentrale Struktur hat sich bewährt und entspricht den Anforderungen, um die mit dem Bundesmeldegesetz beabsichtigten politischen Ziele (u. a. funktionierendes Rückmeldeverfahren, Konsolidierung der Daten, Aktualität der Daten, Nutzung der Meldedaten durch öffentliche Stellen, Online-Melderegisterauskunft und zeitnaher Zugriff auf Meldedaten durch Polizeibehörden) zu erreichen. Der Aufbau eines zentralen Bundesmelderegisters und die damit verbundene problematische, mehrfache Datenhaltung ist daher nicht erforderlich.

Nach dem Entwurf sollen die in den Melderegistern gespeicherten die Identifikation des Betroffenen ermöglichenden Ordnungsmerkmale auch an andere Behörden und öffentlich-rechtliche Religionsgesellschaften übermittelt werden dürfen. Die Ordnungsmerkmale sollen von den Meldebehörden aus den zur jeweiligen Person gespeicherten Meldedaten erstellt werden dürfen und die Führung der automatisierten Melderegister vereinfachen. Im Bundesmelderegister wird zudem ein weiteres Ordnungsmerkmal kreiert, das dem bundesweiten Datenaustausch dienen soll. So entstehen ein oder sogar mehrere verknüpfte einheitliche Personenkennzeichen. Die vorgesehene Schaffung und Verwendung von Ordnungsmerkmalen ist mit den Anforderungen des BVerfG im sog. Volkszählungsurteil nicht zu vereinbaren und daher ebenfalls abzulehnen.

Der Referentenentwurf sieht im Vergleich zu den bislang geltenden Bestimmungen des Melderechtsrahmengesetzes des Bundes und auch denen des bremischen Meldegesetzes eine Ausweitung des Umfangs der von den Meldebehörden zu speichernden Daten und der möglichen Datenübermittlungen vor, die nicht akzeptabel ist. So sollen die Meldebehörden nach dem Referentenentwurf künftig wesentlich mehr Angaben zu ihren Annexkompetenzen, wie z. B. die Mitwirkung bei Steuerverfahren, speichern. Angaben zu Sterbetag und Sterbeort sollen bereits im Rahmen der „einfachen Melderegisterauskunft", bei der es ausreicht, den Betroffenen hinreichend zu bestimmen, erteilt werden dürfen. War z. B. bei der Erteilung von Melderegisterauskünften über eine Vielzahl nicht namentlich bezeichneter Einwohnerinnen und Einwohner (Gruppenauskunft) die für die Zusammensetzung der Personengruppe heranziehbare Angabe „Familienstand" beschränkt darauf, ob verheiratet oder eine Lebenspartnerschaft führend, so sollen nach dem Gesetzesentwurf auch die Kriterien „ledig", „verwitwet" oder „geschieden" maßgeblich sein können. Wie bislang schon nach den Bestimmungen des Melderechtsrahmengesetzes und des bremischen Meldegesetzes soll auch die Übermittlung besonderer Arten personenbezogener Daten, insbesondere von Staatsangehörigkeiten, an Personen, die nicht Betroffene sind, und nicht öffentliche Stellen erlaubt sein, wenn lediglich ein berechtigtes Interesse beim Datenempfänger vorliegt. Dies ist mit den einzuhaltenden datenschutzrechtlichen Anforderungen nicht zu vereinbaren.

Die Rechte der Betroffenen werden mit den Regelungen des Gesetzesentwurfs nicht im erforderlichen Umfang gestärkt. An der Widerspruchslösung bei Datenübermittlungen wird festgehalten anstatt diese durch Einwilligungslösungen zu ersetzen. Auf diese Weise könnte z. B. die Weitergabe von Daten zu Marketingzwecken unterbunden bzw. restriktiv geregelt und Missbräuchen entgegengewirkt werden. Auch die Möglichkeit, Firmen von Datenübermittlungen auszuschließen, wenn sie die ihnen übermittelten Daten missbräuchlich verarbeitet oder genutzt haben, sieht der Gesetzesentwurf nicht vor. Die von Datenschutzbeauftragten schon seit Längerem erhobene Forderung, Melderegisterauskünfte in besonderen Fällen, also z. B. im Zusammenhang mit Alters- oder Ehejubiläen oder für die Herausgabe eines Adressbuchs, nur noch mit der Einwilligung der Betroffenen zu erlauben, bleibt im Entwurf ebenfalls unberücksichtigt.

Für die regelmäßige Übermittlung personenbezogener Daten, insbesondere in Form automatisierter Datenabrufe, bedarf es präziser Festlegungen des Anlasses und des Zwecks der Übermittlungen, der Datenempfänger und der zu übermittelnden Daten, was durch Bundes- oder Landesrecht (z. B. durch Meldedatenübermittlungsverordnung) bestimmt sein muss. Mit der Einrichtung regelmäßiger Datenübermittlungen sind erheblich mehr Risiken verbunden als bei einzelnen nicht regelmäßigen Übermittlungen. Dies gilt auch für die Weitergabe von Daten innerhalb derselben Verwaltungseinheit, z. B. der Kommune. Der Gesetzesentwurf entspricht auch diesen Anforderungen nicht ausreichend.

Im Entwurf fehlen außerdem insbesondere Vorschriften zur wirksamen Protokollierung und Revision. Internetzugänge dürfen nur eingerichtet werden, wenn durch geeignete technische Maßnahmen ein Datenmissbrauch ausgeschlossen ist. Das ist nach den bisherigen Regelungen nicht gewährleistet.

Auch die nach dem Entwurf geplanten Einschränkungen der Prüfkompetenz der Landesdatenschutzbeauftragten aus Gründen der inneren Sicherheit sind absurd und widersprechen der vom Bundesverfassungsgericht immer wieder geforderten effektiven unabhängigen Kontrollmöglichkeit jeglicher personenbezogener Datenverarbeitung.

9.5 Videoüberwachung auf der „Discomeile“

Im Juli 2008 habe ich eine Kontrolle der polizeilichen Videoüberwachung der „Discomeile“ durchgeführt (vgl. 30. JB, Ziff. 9.2). Meine Prüfung ergab, dass die Kennzeichnung des videoüberwachten Bereichs nicht ausreichend ist. Auf dem Weg vom Herdentorsteinweg zur Fußgängerzone „Auf der Brake“ fehlt ein erkennbarer Hinweis auf eine Videoüberwachung. Hier wurde gegen § 29 Abs. 3 Satz 1 Bremisches Polizeigesetz (BremPolG) verstoßen. Es ist hier noch ein weiteres Schild für den Bereich der Kamera „Auf der Brake“ aufzustellen, wie schon aus dem Beschilderungskonzept hervorgeht. Die Polizei holte diesbezüglich eine Erlaubnis des Gebäudeeigentümers ein, um am Überbau des Hauses beim Durchgang Herdentorsteinweg/Auf der Brake ein Schild anbringen zu dürfen. Die Beschilderung soll nun unverzüglich erfolgen. Weiterhin stellte ich fest, dass die Kamera auf dem Rembertiring (in der Nähe der Schilderbrücke, auf der Höhe des Stubu) die Straßenseite des Tivolihochhauses und damit hilfesuchende Drogenabhängige, die das Kontakt- und Beratungszentrum „Tivoli“ aufgesucht haben, filmen konnte. Auch hier lag ein Verstoß gegen § 29 Abs. 3 Satz 1 BremPolG vor. Nach meinem Hinweis wurde dieser Straßenabschnitt von der Kameraüberwachung sofort ausgenommen. Des Weiteren war aufgrund einer fehlerhaften Konfiguration im Zusammenhang mit einem Software-Update das Netz zur Übertragung der Videodaten mit dem bremischen Verwaltungsnetz (BVN) und darüber auch mit dem Internet verbunden. Zwar war es nicht möglich, aus dem BVN oder Internet auf die Kameras und das Netz zur Übertragung der Videodaten zuzugreifen, die Kopplung mit dem BVN widerspricht allerdings dem Sicherheitskonzept für die Videoüberwachung der „Discomeile“. Dieser Fehler wurde nach meinem Hinweis unverzüglich von der Brekom als technischem Betreiber des Netzes beseitigt.

Im Zusammenhang mit der „Discomeile“ erreichten mich Beschwerden betreffend die private Videoüberwachung innerhalb einer Diskothek auf der „Discomeile“. In dieser Diskothek wird auch eine private Videoüberwachung der Notausgänge und des mit den Notausgängen verbundenen Treppenhauses eines privaten Wohngebäudes betrieben. Im Rahmen meiner Prüfung hat es Gespräche mit dem Diskothekenbetreiber, dem Wohnhauseigentümer und dem Stadtamt gegeben, und es wurden Lösungen erarbeitet.

9.6 Aktualisierte KpS-Richtlinien

In meinem 28. Jahresbericht (vgl. Ziff. 9.7) hatte ich die Überarbeitung der aus dem Jahre 1981 stammenden Richtlinien für die Führung Kriminalpolizeilicher Sammlungen (KpS-Richtlinien) gefordert. Diese legen allgemein für typische Sachverhalte der polizeilichen Arbeit fest, welche personenbezogenen Daten erhoben und gespeichert werden dürfen. Darüber hinaus enthalten die KpS-Richtlinien grundlegende Regelungen u. a. zur Übermittlung personenbezogener Daten, zur Auskunft an Betroffene und zur Speicherungsdauer. Die Rechtsgrundlagen für die KpS-Richtlinien finden sich im Bremischen Polizeigesetz (BremPolG), im Bremischen Datenschutzgesetz (BremDSG) und in der Strafprozessordnung (StPO).

Im Mai 2008 wurde mir ein überarbeiteter Entwurf der KpS-Richtlinien vorgelegt, zu dem ich abschließend Stellung nahm. Die neuen KpS-Richtlinien wurden vom Senator für Inneres und Sport zum 1. November 2008 in Kraft gesetzt. Für die Betroffenen konnten einige Vorteile erreicht werden. So wurden die Löschfristen verkürzt. Zum Beispiel bei den Delikten von Jugendlichen mit geringer Bedeutung wurde die Löschfrist von fünf auf zweieinhalb Jahre und bei Kindern von zwei auf ein Jahr halbiert. Die Schadensgrenze bei Sachbeschädigung (§ 303 StGB), Diebstahl (§ 242 StGB), Unterschlagung (§ 246 StGB), Betrug (§ 263 StGB), Erschleichen von Leistungen (§ 265 a StGB) wurde von 100 € auf 1000 € erhöht. Der Grund

für diese Heraufsetzung der Schadensgrenze liegt darin, den Bereich der Kleinkriminalität unterhalb dieser Grenze herauszunehmen. Die personenbezogenen Hinweise (PHW) werden grundsätzlich nach fünf Jahren gelöscht.

Während die anderen Punkte abgestimmt werden konnten, konnte keine inhaltliche Einigung bei dem PHW „psychisch auffällig“ erzielt werden. Die PHW dienen vor allem der Eigensicherung der Polizei (vgl. 30. JB, Ziff. 9.19) und werden im Rahmen der Einsatztaktik der Polizei berücksichtigt. PHW sind beispielsweise Attribute wie „gewalttätig“, „bewaffnet“ oder „psychisch auffällig“. Der letztgenannte PHW wird bundesweit nur im Land Bremen nach der Dienstanweisung über polizeiliche Maßnahmen gegenüber psychisch auffälligen Personen aus dem Jahre 2003 vergeben. In dieser Dienstanweisung wird geregelt, dass der PHW „psychisch auffällig“ im Vorfeld der Feststellung einer psychischen Krankheit vergeben werden kann. Somit bedarf es für diesen Eintrag in dem polizeilichen Informationssystem keiner Feststellung einer psychischen Erkrankung durch den Arzt.

Beschwerden von Betroffenen führten dazu, dass die Vergabe des PHW „psychisch auffällig“ im jeweiligen Einzelfall nicht genau verifizierbar war (vgl. 30. JB, Ziff. 9.5 und Ziff. 9.19). Mit Blick auf die bundesweit durchaus übliche Vergabe eines PHW „psychisch krank“ nach ärztlicher Feststellung regte ich an, den PHW „psychisch auffällig“ abzuschaffen und den PHW „psychisch krank“ einzuführen. Inwieweit darüber hinaus noch eine weitere Kategorie erforderlich ist, die den Kreis der Eigen- und Fremdgefährder ohne ärztliche Feststellung umfasst, bedarf noch weiterer Erörterung.

9.7 Internetnutzung bei der Polizei Bremen

Vor vier Jahren habe ich die Internetnutzung bei der Polizei Bremen geprüft und aufgrund der vorgefundenen Mängel ein entsprechendes Datenschutzkonzept gefordert, das den Einsatz von Rechnern mit Internetanschlüssen in den Revieren regelt (vgl. 27. JB Ziffer 6.1). Da bei der Polizei Bremen der Zugriff auf das Programm Fundinfo über eine Internetverbindung geplant ist (vgl. 29. JB Ziffer 9.21), habe ich es für erforderlich gehalten, die Umsetzung der von der Polizei Bremen seinerzeit angekündigten Maßnahmen zu überprüfen. Dazu habe ich die Internetnutzung in zwei Polizeirevieren sowie in zwei Abteilungen des Polizeipräsidiums geprüft.

Polizeiinterne Vorgaben für die Mitarbeiter zur Nutzung des Internets ergeben sich aus der „Dienstanweisung für die Nutzung des Internet bei der Polizei Bremen“. Danach ist die private Nutzung des Internets untersagt. Weiterhin ist es nicht zulässig, Daten mit dienstlichem Bezug auf den Internetrechnern zu speichern. Die Dienstanweisung sowie ein weiteres Merkblatt zur Internetnutzung wurden auf dem Desktop eines jeden Internetrechners sichtbar für die Mitarbeiter zur Verfügung gestellt. Die Revier- und Abteilungsleiter vor Ort haben mir bestätigt, dass allen Mitarbeitern die Regelungen zur Internetnutzung bekannt seien.

Die seinerzeit bestehende Standalone-PC-Lösung für die Internetnetnutzung wurde inzwischen abgelöst. Die eingesetzten Internetrechner werden jetzt zentral administriert und automatisiert gewartet. Es wurde ein zweistufiges Anmeldeverfahren implementiert. Die Mitarbeiter haben keine Administrationsrechte mehr. Entgegen meiner Empfehlung, externe Medien, wie z. B. CD-Laufwerke, zu deaktivieren und USB-Schnittstellen zu sperren, sind diese allerdings weiterhin uneingeschränkt zur Nutzung freigegeben worden.

Meine Prüfung der Festplatteninhalte hat ergeben, dass aufgrund der vorgefundenen Dateien und Cookies auf eine private Nutzung zu schließen ist. So sind beispielsweise PC-Spiele, ein Programm zur Musikbearbeitung, Kirchengemeindebriefe und Dokumentationen zu Ausbildungsberufen vorgefunden worden, wie auch zahlreiche Bilddateien mit Familienfotos, Tierfotos, Grundrisse von Häusern, Skulpturen, Rasenmähern, Grillbauten, Motorrädern, Angeln, Fußballveranstaltungen sowie Cookies von Urlaubsgebieten, Videoportalen, Mitfahrzentralen, Veranstaltungsportalen und Interneteinkaufsshops.

Bei einigen Programmen ist derzeit noch unklar, ob diese in Kenntnis und mit Zustimmung der Abteilung Informations- und Kommunikationstechnik heruntergeladen worden sind. Hierbei handelt es sich u. a. um Google Earth, einen freien Virenscanner, Bildbetrachtungsprogramme, Tools für den Einsatz von Festplatten und USB-Sticks sowie Software zum Brennen von CDs.

An unzulässigen dienstlichen Daten habe ich Bilder einer Überwachungskamera vorgefunden. Außerdem sind auf einem Rechner Personalstatistiken der Polizei Bremen bearbeitet worden.

Die private Nutzung des Internets stellt einen klaren Verstoß gegen die Dienstanweisung dar. Nach Ziffer 3.5 ist eine private Nutzung unzulässig. Aber selbst, wenn in Zukunft die private Nutzung bei der Polizei Bremen gestattet werden sollte, ist zu beachten, dass nach Ziffer 4 Absatz 3 der Richtlinie für die Bereitstellung und Nutzung von Internet-/Intranetzugängen vom 1. Februar 2004 (BremABl. Nr. 20 vom 10. Februar 2004) das Handeln der Mitarbeiter der Polizei Bremen insofern unzulässig wäre, als dass hier Dateien, wie z. B. PC-Spiele, und andere ausführbare Dateien heruntergeladen worden sind.

Die Installation bzw. das Herunterladen von nicht zugelassen Programmen und Dateien kann die Sicherheit des Systems gefährden. Der geplante Einsatz des Programms Fundinfo bei der Polizei Bremen ist so lange datenschutzrechtlich bedenklich, wie nicht sichergestellt ist, dass eine solche Nutzung der Rechner unterbleibt. Die Mitarbeiter müssen daher nochmals im Hinblick auf den Umgang mit dem Internet und den damit verbundenen Gefahren sensibilisiert werden.

Bereits bei der letzten Prüfung der Internetrechner habe ich darauf gedrungen, dass keine dienstlichen personenbezogenen Daten auf den Internetrechnern gespeichert werden. Wegen der besonderen Risiken bei der Nutzung des Internets (z. B. Verlust der Vertraulichkeit und der Integrität) ist nach Ziffer 6. der Dienstanweisung für die Nutzung des Internets der Polizei Bremen das Speichern von Daten mit dienstlichem Bezug auf Internetrechnern nicht gestattet. Es sollte daher nochmals darauf hingewirkt werden, zukünftig eine Speicherung personenbezogener dienstlicher Daten auf diesen Rechnern zu verhindern.

Da in keinem Fall eine Begründung für eine Nutzung externer Medien genannt werden konnte, empfehle ich, die Medien zu deaktivieren und nur in konkreten Einzelfällen eine dedizierte Nutzung der USB-Schnittstelle zu erlauben.

Meine Prüfberichte habe ich der Polizei Bremen übersandt. Eine Stellungnahme steht aus.

9.8 PIER

PIER steht für Polizeiliche Information Ermittlung Recherche. Dieses Verfahren soll der Polizei Bremen bei komplexen Ermittlungen zur Seite stehen und insbesondere Beziehungen zwischen verschiedenen Personengruppen visualisieren.

Das System PIER ist mandantenfähig. Geplant sind zwei Mandanten. Wie unter Ziffer 9.9 dieses Jahresberichts beschrieben, werden die Sexualstraftäter aus dem Verfahren HEADS (Haft-Entlassenen-Auskunfts-Datei-Sexualstraftäter) als ein Bestandteil in PIER gespeichert. Dies soll in dem einen Mandanten erfolgen, in dem auch weitere Daten, z. B. vom Staatsschutz, bearbeitet werden. Insofern ist datenschutztechnisch durch Berechtigungen eine strikte Abgrenzung erforderlich, die sicherstellt, dass nur auf die erforderlichen Daten in dem jeweiligen Verfahren zugegriffen werden kann. Aus dem Berechtigungskonzept geht hervor, dass es unterschiedliche Rollen (z. B. Administrator, Sachbearbeiter, Dolmetscher) gibt. Es ist zurzeit unklar, ob diese strikte Trennung innerhalb eines Mandanten eingehalten werden kann bzw. wie groß das Risiko ist, dass durch fehlerhafte Berechtigungsvergabe auf sensible Daten eines anderen Moduls innerhalb eines Mandanten zugegriffen werden kann. Eine klare Trennung zwischen den Modulen Staatsschutz und HEADS wäre aus datenschutzrechtlicher Sicht die bessere Lösung.

Eine besondere Funktion dieses Programms ist die Meldungskonfiguration. Sollte in einem Verfahren ein Täter in PIER erfasst werden, der bereits in einem anderen Verfahren in PIER erfasst worden ist, so werden grundsätzlich Meldungen an die beteiligten Verfahren (auch zwischen den beiden Mandanten) generiert. In dem Mandanten, in dem die Daten von HEADS und dem Staatsschutz gespeichert sind, ist durch geeignete Konfiguration sicherzustellen, dass keine Meldungen aus diesem Mandanten in den anderen Mandanten erfolgen.

Zu einer ersten Version der Verfahrensbeschreibung von PIER hatte ich bereits im Juli 2008 Stellung genommen. Aus technischer Sicht habe ich angemerkt, dass noch Angaben zur Zugangs- und Zugriffskontrolle, zur Eingabekontrolle und der Verfügbarkeitskontrolle zu machen sind. Die Verfahrensbeschreibung, die Erfassungs-

richtlinien und das Berechtigungskonzept wurden mir Ende September 2008 in aktualisierter Form vorgelegt und werden derzeit durch mich geprüft. Die Inhalte der Protokollierung sowie die Protokollierungsfristen befinden sich noch in der Abstimmung mit mir.

9.9 HEADS

HEADS ist eine Kurzbezeichnung für Haft-Entlassenen-Auskunfts-Datei-Sexualstraftäter. Sinn und Zweck dieser Datei ist die Überwachung rückfallgefährdeter Sexualstraftäter. HEADS zielt auf den Schutz der Bevölkerung durch eine Minimierung des Risikos einer erneuten Begehung von Straftaten von als besonders rückfallgefährdet eingestuften Sexualstraftätern. Dies soll durch eine Verbesserung des Informationsaustausches zwischen Polizei und Justiz erreicht werden. Beispielsweise soll die Zusammenarbeit zwischen Vollstreckungsbehörde, Justiz-/Maßregelvollzug, Führungsaufsichtsstelle und Bewährungshilfe sowie Polizeibehörden optimiert werden. Dieser Informationsaustausch zwischen Polizei und Justiz beruht auf einem Datenübermittlungs- und Datenverarbeitungsprozess. Zum Konzept dieser Datei habe ich gegenüber dem Senator für Inneres und Sport Stellung genommen. Grundsätzliche rechtliche Bedenken gegen die Einführung dieser Datei habe ich nicht. HEADS wird in PIER (Polizeiliche Informationen Ermittlung Recherche (vgl. Ziff. 9.8 dieses Berichts) geführt.

9.10 ZAKS

Die Zentrale Antikorruptionsstelle (ZAKS) beim Senator für Inneres und Sport ist eine Stelle, bei der jeder Verdacht auf Korruption gemeldet werden kann.

Die Homepage der ZAKS bietet die Möglichkeit, Mitteilungen an die ZAKS per Kontaktformular auf dem E-Mail-Weg zu senden. Hierbei handelt es sich um einen unverschlüsselten Übertragungsweg. Die Hinweisgeberin oder der Hinweisgeber wird nicht darüber informiert, dass es sich um eine unsichere Verbindung handelt, die nicht gegen unbefugte Lesezugriffe auf dem Übertragungsweg geschützt ist. Ich habe nachdrücklich eine Verschlüsselung empfohlen.

9.11 Keine Ermittlungen von Polizeibeamten in eigener Sache

Im Jahr 2008 beschäftigte ich mich weiterhin mit der Thematik unbefugter Abrufe von Polizeibeamten aus dem polizeilichen Informationssystem (ISA-Web) sowie unzulässiger Ermittlungen von Polizeibeamten (vgl. 30. JB, Ziff. 9.5). Abfragen aus dem polizeilichen Informationssystem und Ermittlungen dürfen gemäß § 20 Bremisches Verwaltungsverfahrensgesetz (BremVwVfG) nicht von einem Polizisten vorgenommen werden, der selbst betroffen oder beteiligt ist oder ein Angehöriger eines Beteiligten ist. Betroffen ist ein Polizeibeamter, wenn er außerhalb seiner amtlichen Eigenschaft als Polizist auf sonstige Art und Weise eine Beziehung zur Sache hat. Hierzu zählt z. B. auch die ehrenamtliche Tätigkeit oder Mitgliedschaft in einem Verein. Gründe für die Unzulässigkeit von Abfragen aus ISA-Web oder von Ermittlungen liegen in der Befangenheit und Parteilichkeit des Polizeibeamten. Abfragen aus dem polizeilichen Informationssystem oder Ermittlungen zur Ahndung einer Ordnungswidrigkeit oder Verfolgung einer Straftat, die ein befangener Polizeibeamter durchführt, sind daher unzulässig. Ich habe mich daher mit dem Polizeipräsidenten darauf geeinigt, dass dieser alle Polizeibeamten in Bremen noch einmal auf diese Rechtslage hinweist. Dies ist mit Anweisung vom November 2008 geschehen. Entsprechend habe ich auch die Polizei in Bremerhaven informiert.

9.12 Eingaben im Bereich der Polizei von Bremen und Bremerhaven

Die Eingaben von Bürgern über die Verarbeitung ihrer Daten im polizeilichen Informationssystem haben in den vergangenen Jahren zugenommen. Ich konnte verschiedenen Bürgern helfen, ihre Rechte auf Auskunft, Berichtigung oder Löschung durchzusetzen.

In einem Fall kam es zu einer Verwechselung von Familienangehörigen aufgrund der Namensähnlichkeit. Der Sohn wurde trotz unterschiedlichen Alters und unterschiedlichen Geburtsnamens mit seinem Vater verwechselt. Daten, die den Vater betrafen, wurden beim Sohn gespeichert; sie waren in dem polizeilichen Informationssystem zu löschen. Hier wurde eine Löschung bzw. Berichtigung dieser Einträge durch mich erreicht.

In einem anderen Fall kam ein Petent zu mir und bat um die Löschung kriminalpolizeilicher Daten aus dem polizeilichen Informationssystem ISA-Web. Die Polizei Bremerhaven sah den Zeitpunkt der Verurteilung als für die Fristberechnung maßgeblich an. Fristbeginn ist aber der Tatzeitpunkt und damit die Erfassung bei der Polizei und nicht die Verurteilung, denn die Strafverfahrensdauer darf dem Betroffenen nicht zum Nachteil gereichen. Eine Stellungnahme steht noch aus.

Einer weiteren Beschwerde lag ein Wortgefecht zwischen Bürgern auf offener Straße zugrunde. In dieser Auseinandersetzung behauptete eine Bürgerin, alles über den anderen Bürger zu wissen, denn sie arbeite schließlich bei der Polizei. Ich ging dessen Beschwerde nach. Meine Prüfung ergab, dass die Bürgerin zwar in den Räumen der Polizei arbeitet, es wurde aber keine unbefugte Abfrage in der kriminalpolizeilichen Sammlung vorgenommen.

9.13 Rechtewahrung in gemeinsam genutzten Laufwerken bei der Polizei Bremen

Im Berichtsjahr 2004 bin ich im Rahmen von datenschutzrechtlichen Prüfungen bei der Polizei Bremen auf ein sogenanntes öffentliches Laufwerk aufmerksam geworden, das zum Datenaustausch und zur organisationsübergreifenden Sachbearbeitung betrieben worden ist. Meine datenschutzrechtliche Auffassung habe ich im 27. Jahresbericht unter Ziffer 6.2 dargestellt. Seinerzeit wurde ein öffentliches Laufwerk genutzt, für das es kein Datenschutzkonzept gab. Die Daten konnten von der gesamten Polizei Bremen eingesehen werden, und es gab keine Regelung zur Löschung der dort gespeicherten Dateien. Die danach durch die Polizei Bremen neu geschaffenen Regelungen habe ich in diesem Jahr geprüft.

Die Polizei Bremen hat zwei zentrale Laufwerke eingerichtet. Zum einen steht für Dateien, die aufgrund der Größe nicht über das E-Mail-System ausgetauscht werden sollen, ein öffentliches Laufwerk zur Verfügung. Um zu verhindern, dass Daten über einen längeren Zeitraum ungelöscht gespeichert bleiben, soll wöchentlich automatisiert die Löschung aller hier noch verbliebenen Dateien erfolgen. In diesem Speicherbereich befanden sich zum Zeitpunkt der Prüfung nur wenige Dateien, die jünger waren als das Datum des letzten Löschvorgangs. Die vorgeschriebene Löschung wurde eingehalten.

Zum anderen ist ein Laufwerk eingerichtet worden für Datenzugriffe, die organisationsübergreifend von Mitarbeitern aus mehreren Sachgebieten erfolgen müssen und auf dem jeder Direktion ein eigenes Verzeichnis zugeordnet worden ist.

Die Vergabe von Berechtigungen für diese Unterverzeichnisse ist auf die Direktionen delegiert worden. Jede Direktion hat für diese Aufgabe einen oder mehrere Verantwortliche bestimmt. Die Verantwortlichen haben Vollzugriff und können weitere Unterverzeichnisse anlegen sowie Mitarbeiter zur Nutzung zuordnen.

In der von der Abteilung IuK erstellten Dokumentation wird darauf hingewiesen, dass die Verantwortlichen für ihre Arbeit dokumentationspflichtig sind, dass diese Dokumentation Bestandteil der IT-Revision sein kann und auch aus Datenschutzgründen erforderlich ist.

Ich habe bzgl. der Berechtigungsvergabe kritisiert, dass es keine technischen Möglichkeiten einer revisionssicheren Protokollierung gibt. Die Überprüfung der Dokumentation über die Vergabe der Zugriffsberechtigung auf Verzeichnisse in einer Fachdirektion hat ergeben, dass es keine vollständigen Unterlagen darüber gab, wie die Berechtigungen vergeben worden sind.

Ich habe der Polizei Bremen bereits in 2007 empfohlen, ein Werkzeug zur Dokumentation des Istzustands für die Berechtigungseinstellungen zu nutzen. Auf diese Weise können zunächst einmal grundsätzliche Überprüfungen kritischer Zustände (Vergabe Vollzugriff, Zugriff für Jedermann) durchgeführt werden.

Weiterhin besteht die Möglichkeit, dass anhand dieser Dokumentation die Direktionen zu einer regelmäßigen Überprüfung der aktuellen Berechtigungen angehalten werden. Unklare Berechtigungsvergaben sollen anhand der vollständigen Aufbewahrung der Anträge geklärt werden.

Die Polizei Bremen hat mitgeteilt, dass sie mittlerweile den Istzustand über ein Snapshotverfahren rudimentär speichert. Diese Dokumentation ist allerdings auch für einen Soll-/Istvergleich der Berechtigungen nur sehr eingeschränkt verwendbar. Daher ist die Polizei Bremen in Kontakt mit dem Hersteller ihres proprietären Betriebssystems getreten, um eine brauchbare Dokumentationslösung zu erhalten.

Diese Vorgehensweise stellt insgesamt eine schwächere Form gegenüber einer automatisierten Protokollierung dar.

9.14 Das normenverdeutlichende Gespräch mit Kindern und Jugendlichen

Die Polizei Bremen möchte Gespräche mit Kindern und jugendlichen Ersttätern führen, um den Minderjährigen das Unrecht der Tat vor Augen zu führen. Auch deren Erziehungsberechtigte sollen mit einbezogen werden, um diese auf ihre Verantwortung im Sozialisierungsprozess hinzuweisen und sie zur Wahrnehmung ihrer Pflichten gemäß Art. 6 Grundgesetz (GG), § 171 Strafgesetzbuch (StGB) und §§ 52 bis 58 Bremisches Schulgesetz (BremSchulG) anzuhalten. Vor den Gesprächen möchte die Polizei die kriminalpolizeilichen Informationssysteme abfragen und dabei neben den Kindern und jugendlichen Ersttätern auch die Eltern überprüfen. Über Art und Ausgestaltung des Verfahrens finden derzeit Gespräche mit der Polizei statt.

9.15 ViCLAS-Datenbank des Bundeskriminalamtes

Auch in diesem Jahr ist mir vom Bundesministerium des Innern die Errichtungsanordnung „ViCLAS“ zur automatisierten Datei mit personenbezogenen Daten beim Bundeskriminalamt (§ 34 BKAG) zur Stellungnahme gegenüber dem Senator für Inneres und Sport übersandt worden. Derzeit findet grundsätzlich eine lokale Speicherung von Daten über Straftaten von Kindern in der kriminalpolizeilichen Sammlung statt, die das 7. Lebensjahr vollendet haben. Die ViCLAS-Datenbank ist ein Instrument zur Abbildung von Straftaten und Täterverhalten im Bereich der sexuell motivierten Gewaltkriminalität (Tötungs- und Sexualdelikte). In dieser bundesweiten Verbunddatei sollen Kinder als Täter gespeichert werden. Ich habe Bedenken gegen die Eröffnung einer bundesweiten Zugriffsmöglichkeit auf die dort gespeicherten Daten von Kindern, weil bisher nicht hinreichend nachgewiesen ist, dass die in Rede stehenden Kinder überörtlich tätig werden. Ich habe mich daher mangels rechtlicher Erforderlichkeit gegen die Erweiterung der Speicherung von Daten über strafunmündigen Kindern auf Bundesebene ausgesprochen.

9.16 Bericht aus dem Arbeitskreis Sicherheit

Der Arbeitskreis Sicherheit der Datenschutzbeauftragten des Bundes und der Länder dient dem Erfahrungs- und Informationsaustausch. Aus der Fülle der Themen seien folgende exemplarisch genannt: HEADS (Haft-Entlassenen-Auskunfts-Dateirückfallgefährdeter-Sexualstraftäter [vgl. Ziff. 9.9 dieses Berichts]), die Zuverlässigkeitsüberprüfungen, die polizeiliche Überwachung von Internetknotenpunkten, der Datenschutz in der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene, das Bundeskriminalamtgesetz (vgl. Ziff. 20.1), die Antiterrordatei (vgl. Ziff. 9.18) , die Praxis der Auskunftserteilung durch die Polizei und die Auskunftspraxis bei den Verfassungsschutzbehörden.

9.17 Onlinedurchsuchung privater Computer

Bahnbrechend ist die Entscheidung des Bundesverfassungsgerichts (BVerfG) vom 27. Februar 2008 (Az. 1 BvR 370/07; 1 BvR 595/07) zur Onlinedurchsuchung. Gegenstand des Verfahrens vor dem BVerfG waren Verfassungsbeschwerden gegen das Gesetz über den Verfassungsschutz in Nordrhein-Westfalen, welches zum einen Befugnisse der Verfassungsschutzbehörde zu verschiedenen Datenerhebungen aus informationstechnischen Systemen, gemeint sind insbesondere private Computer, zum anderen den Umgang mit den erhobenen Daten vorsah. Im Fokus ist eine Vorschrift, die zum heimlichen Zugriff auf informationstechnische Systeme ermächtigt, die sogenannte Onlinedurchsuchung.

Das BVerfG hat diese Vorschrift für „verfassungswidrig und nichtig“ (Rn. 165) erklärt. Die Vorschrift zur Onlinedurchsuchung verletze das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz [GG]) in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Rn. 166). Diese Ausprägung des allgemeinen Persönlichkeitsrechts schützt vor Eingriffen in informationstechnische Systeme, soweit der Schutz nicht durch andere Grundrechte wie Art. 10 GG (Telekommunikationsgeheimnis), Art. 13 GG (Unverletzlichkeit der Wohnung) oder durch das Recht auf informationelle Selbstbestimmung gewährleistet ist (Rn. 167). Das BVerfG stellt fest, dass die Vorschrift zur Onlinedurchsuchung nicht dem Ge-

bot der Normenklarheit genügt (Rn. 208), die Anforderungen des Verhältnismäßigkeitsgrundsatzes nicht gewahrt sind (Rn. 218) und die Norm keine hinreichenden Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung enthält (Rn. 167). Das BVerfG entwickelte damit ein neues Grundrecht auf Gewährleistung und Integrität informationstechnischer Systeme (Rn. 201), um den neuartigen Gefährdungen im Zuge des informationstechnischen Fortschritts und gewandelter Lebensverhältnisse Rechnung zu tragen (Rn. 169 und 187). Es dient dem Schutz der Privatsphäre. Die Anforderungen, die das BVerfG aufstellt, wie zum Beispiel die Verfahrensvorkehrungen, der Vorbehalt richterlicher Anordnung, haben auch Geltung für den Gesetzentwurf zur Abwehr des internationalen Terrorismus (vgl. Ziff. 9.19 dieses Berichts).

9.18 Prüfung der Antiterrordatei

Im September und Oktober 2008 habe ich eine Ergänzungsprüfung der Antiterrordatei beim Landeskriminalamt (LKA) und beim Landesamt für Verfassungsschutz (LfV) durchgeführt (vgl. 30. JB, Ziff. 9.6). Eine Aktualisierung der Antiterrordatei findet wöchentlich statt. Ich habe stichprobenartig verschiedene Datensätze überprüft. Des Weiteren habe ich das Verfahren bei Abrufen und Eilabrufen von Bundesbehörden hinsichtlich erweiterter Grunddaten im Sinne des Antiterrordateigesetzes (ATDG) vom 22. Dezember 2006 kontrolliert. Von der Einhaltung der Vorgaben des ATDG habe ich mich vor Ort überzeugt. Eine Kontrolle der Protokolldaten steht noch aus.

9.19 Abwehr des internationalen Terrorismus

Der Gesetzentwurf zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (BKAG-E; BT-Drs. 16/9588, 16/10121 und 16/10822) führte zu heftigen Diskussionen. Wesentliche Kritikpunkte, die u. a. auch vom Deutschen Anwaltverein, der Bundesrechtsanwaltskammer und vom Deutschen Journalisten-Verband vorgebracht werden, bestehen in der Ausweitung der präventiven Befugnisse des Bundeskriminalamts (BKA). Ermächtigungen, wie zum Beispiel die Rasterfahndung (vgl. 29. JB, Ziff. 9.2), die Onlinedurchsuchung von privaten PC (vgl. Ziff. 9.17 dieses Berichts), der Spähangriff in Wohnungen oder die Herausgabepflicht von Daten der Informanten durch Journalisten, sind unangemessen. Bedenken bestehen darüber hinaus hinsichtlich der Datenvorsorge zur Verfolgung künftiger Straftaten. Der Schutz von Daten aus dem Kernbereich privater Lebensgestaltung wird faktisch, beispielsweise durch die Regelung über Lausch- und Spähangriffe gemäß § 20 h Abs. 5 BKAG-E, unterlaufen.

Als weiterer grundsätzlicher Kritikpunkt wird die Verschiebung der Sicherheitsarchitektur genannt. Die Grenzen zwischen nachrichtdienstlichen Erkenntnissen und kriminalpolizeilichen Prognosen und Handlungsgrundlagen werden verwischt. Dies wird auch als sogenannte Vernachrichtlichung bezeichnet. An dieser Stelle wird gegen das verfassungsrechtliche, rechtsstaatliche Trennungsgebot verstoßen. Kritik muss auch an der Unbestimmtheit und damit der mangelnden Normenklarheit geübt werden. Der Begriff des internationalen Terrorismus wird nicht gesetzlich definiert. Die Zuständigkeiten von BKA und LKA können nicht klar abgegrenzt werden. Parallelzuständigkeiten und damit einhergehende Ermittlungspannen sind zu befürchten. Die Evaluierung von fünf Jahren ist zu lang. Stattdessen ist eine Befristung der Befugnisse anzustreben. Abgeordnete von Oppositionsparteien haben Verfassungsbeschwerden gegen diesen Gesetzentwurf angekündigt.

9.20 Unfalldatenschreiber bei der Feuerwehr

Bei der Feuerwehr in Bremen und Bremerhaven werden sogenannte Unfalldatenspeicher (UDS) eingesetzt. Ein Unfalldatenspeicher ist ein Gerät, welches bei Inbetriebnahme des Rettungsfahrzeugs permanent und uhrzeitgenau Fahrzeugbewegungen, Stellung bzw. Bedienung angeschlossener Bedienelemente erfasst und interne Vorgänge überwacht.

Die Einführung dieser Geräte habe ich in 2005 bei der Feuerwehr in Bremen begleitet (vgl. 28. JB, Ziff. 9.13). Nach einem Probebetrieb habe ich Ende 2006 die Überprüfung der technischen und organisatorischen Maßnahmen bei der Feuerwehr Bremen vorgenommen. Daraus ergaben sich einige Forderungen zur Verbesserung des Datenschutzes, beispielsweise eine Festplattenverschlüsselung für das Notebook, Vorgaben zur Protokollierung und zum Anmeldeverfahren, dessen Um-

setzung die Feuerwehr Bremen nachträglich vornahm. Eine Überprüfung der Ereignisdaten des UDS konnte seinerzeit nicht vorgenommen werden, da diese inkonsistent waren. Eine nachträgliche Kontrolle dieser Ereignisdaten bei der Feuerwehr in Bremen fand im Juli 2008 statt. Der zum Auslesen eines UDS erforderliche Laptop wurde verschlossen aufbewahrt und enthielt die ausgelesenen Daten sowie die erforderliche Software. Die Auswertung der Ereignisdaten, wie zum Beispiel Blaulicht, Blinker rechts/links, Bremse und Sirene im Statistikspeicher, automatischen Speicher und Stillstandspeicher, ergab, dass bisher kein Auslesen stattfand und die Daten konsistent waren.

Ein besonderes Augenmerk richtete ich auf rechtliche Fragen des Arbeitnehmerdatenschutzes. Durch das Auslesen der Daten eines UDS können Verhaltensanalysen hinsichtlich der im Rettungsdienst tätigen Fahrerinnen und Fahrer durchgeführt werden. Ein Auslesen zu diesem Zweck ist nicht erlaubt. Durch Dienstvereinbarungen bei den Feuerwehren in Bremen und Bremerhaven sowie bei den verschiedenen Rettungsdiensten Arbeiter-Samariter-Bund, Deutsches Rotes Kreuz und Malteser wird gewährleistet, dass ein Auslesen des UDS nicht ohne Kenntnis der Fahrerin bzw. des Fahrers des Rettungsfahrzeugs vorgenommen wird. Insofern wird dem Datenschutz für den Bereich der Arbeitnehmerinnen und Arbeitnehmer ausreichend Rechnung getragen.

9.21 Elektronischer Personalausweis kommt 2010

Der neue elektronische Personalausweis soll 2010 im Scheckkartenformat eingeführt werden. Die gesetzliche Grundlage ist das Gesetz über Personalausweise und den elektronischen Identitätsnachweis (PAG, BT-Drs. 16/10489 vom 7. Oktober 2008). Er vereint drei Funktionen in einem. Neben der bisher gebräuchlichen Ausweisfunktion, zum Beispiel für die Reise, treten die Identitätsfunktion für das E-Government und E-Business sowie optional die Signaturfunktion als elektronisches Pendant zur eigenhändigen Unterschrift. Der neue elektronische Personalausweis wird mit einem RFID-Chip versehen sein, auf dem die persönlichen Daten des Ausweisinhabers inklusive Lichtbild und auf Wunsch zwei Fingerabdrücke gespeichert werden. Es sind aber noch eine Reihe datenschutzrechtlicher Fragestellungen offen.

Aus dem Grobkonzept des Bundesministeriums des Innern (BMI) zum elektronischen Personalausweis (Version 2.0) geht hinsichtlich der Sicherheit der Biometriedaten nicht klar hervor, wie diese auf dem Chip gegen unberechtigtes Auslesen gesichert werden sollen. Hinsichtlich der Verwendung der Identitätsfunktion im Internet bestehen Gefahren durch Schadsoftware auf dem PC des Bürgers. Hier ist ein Abhören des Datenflusses oder ein Auslesen der PIN möglich. Zur Schadensminimierung darf die Kommunikation nur über eine gesicherte Datenleitung (Datenkanal) betrieben werden. Nicht geklärt ist, wer im Schadensfall haftet. Ein weiterer Kritikpunkt wird im Grobkonzept hinsichtlich der Integration von Zertifikaten und Schlüsseln beschrieben, die als eindeutige Personenkennzeichen für die Gültigkeitsdauer des Personalausweises verwendet werden können. Es sind Regelungen zur Seriennummer und äquivalente Vorkehrungen zum Schutz des allgemeinen Persönlichkeitsrechts zu treffen. Diese Vorkehrungen müssen näher bezeichnet werden. Des Weiteren muss geregelt sein, wie verfahren werden soll, wenn der RFID-Chip defekt ist. Die drei Funktionen des neuen Ausweises müssen datenschutztechnisch getrennt zur Verfügung gestellt werden. Gefahren bestehen im Hinblick auf die Manipulation von sehr sensiblen Daten, wie zum Beispiel das biometrische Lichtbild, und den Diebstahl von Identitäten. Des Weiteren habe ich zusammen mit den anderen Datenschutzbeauftragten des Bundes und der Länder datenschutzrechtliche Bedenken gegen die Speicherung der Fingerabdrücke auf dem RFID-Chip geäußert. Nach den Verhandlungen der Datenschutzbeauftragten mit dem BMI wurde diese Wahlmöglichkeit hinsichtlich der Speicherung von Fingerabdrücken erreicht.

9.22 Projekt „Unbarer Zahlungsverkehr“ für die Verwaltung

In der gesamten bremischen Verwaltung ist die Möglichkeit eines unbaren Zahlungsverkehrs geplant. Dabei soll mit externen Diensteanbietern zusammengearbeitet werden. Seit 2007 wird dieses Projekt (früher „Bargeldloser Zahlungsverkehr für Verwarnungen“) durch mich beraten.

Von besonderem Interesse ist, dass ein externer Provider beauftragt werden soll, sich um die Zahlungseingänge zu kümmern und bestimmte Zahlungsdaten zu

archivieren. Diese Beauftragung zur Abwicklung des unbaren Zahlungsverkehrs stellt eine Auftragsdatenverarbeitung nach § 9 Bremisches Datenschutzgesetz (BremDSG) dar, dessen Vorgaben zu berücksichtigen sind. Die datenschutzrechtliche Verantwortlichkeit verbleibt gemäß §§ 9 Abs. 1 Satz 1, 2 Abs. 3 Nr. 1 BremDSG beim Auftraggeber. Konkret haben Auftragnehmer also mit den Auftragsunterlagen schriftlich darzustellen:

— die Datenverarbeitung (Geschäftsprozessmodellierung nebst Datenübermittlungen),

— ggf. die Unterauftragsverhältnisse (Einschaltung Dritter zur Auftragsabwicklung),

— die technischen und organisatorischen Maßnahmen nach § 7 BremDSG (z. B. in Gestalt eines IT-Sicherheitskonzepts oder Datenschutzkonzepts) und

— ggf. meine Kontrollmöglichkeiten sicherzustellen.

Die sichere Zahlungsabwicklung setzt verschiedene technische und organisatorische Maßnahmen des Auftragnehmers voraus. Hierzu gehören etwa die sichere Authentifizierung an Geräten und Software, eine verschlüsselte Übertragung der Zahlungsdaten sowie Plausibilitätsprüfungen und Protokollierungen. Zur Routine gehört es sicherzustellen, dass beim Auftragnehmer nur Befugte Zugang und Zutritt zu den Datenverarbeitungsanlagen und Zugriff auf die Abrechnungsdaten besitzen und dass Zugriffe revisionssicher protokolliert werden. Im Rahmen der Verfügbarkeitskontrolle ist zu gewährleisten, dass beispielsweise die Belege für die Speicherdauer zum Zwecke der Rechnungsprüfung lesbar bleiben.

Es ist durch geeignete Maßnahmen sicherzustellen, dass bei unbarer Zahlung zum Beispiel die Art der Verwarnung nicht elektronisch übermittelt wird oder gar auf dem Konto- oder Kreditkartenbeleg der Überweisenden erscheint. Der Zahlungsbeleg muss einem konkreten Vorgang zuordenbar bleiben, zum Beispiel bei Nachfragen des Bürgers oder zum Nachvollziehen der Verbuchung.

Es besteht ein schutzwürdiges Interesse der Betroffenen, nicht unter Verwendung unbarer Zahlungsmethoden bezahlen zu müssen, die weitere, möglicherweise ungewollte Datenspuren, zum Beispiel auf dem Konto oder der Kreditkartenabrechnung, auslösen. Den betroffenen Bürgern muss daneben eine bare und damit anonyme Zahlungsmöglichkeit verbleiben. Auf die Freiwilligkeit der unbaren Zahlung, die dann nur mit Einwilligung gemäß § 3 Abs. 3 und 4 BremDSG der Betroffenen erfolgen darf, ist in geeigneter Form hinzuweisen; dies geschieht in der Verwaltung regelmäßig per Dienstanweisung.

10. Justiz

10.1 Prüfung des Medizinischen Dienstes der Justizvollzugsanstalt Bremen

Im Juli 2008 habe ich den Medizinischen Dienst der Justizvollzugsanstalt (JVA) Bremen einer datenschutzrechtlichen Prüfung unterzogen. Gegenstand der Prüfung war die Verarbeitung von Patientendaten in rechtlicher Hinsicht.

Der Medizinische Dienst der JVA ist für die medizinische Versorgung von Strafgefangenen zuständig. Bei Aufnahme eines Strafgefangenen wird dieser durch den Medizinischen Dienst untersucht. Es wird hierbei u. a. die Tauglichkeit des Häftlings für Vollzug, Einzelunterbringung, Arbeiten, Reise- oder Beförderungsfähigkeit oder Erwerbsbeschränkung festgestellt. Weitere Untersuchungen finden dann nur noch anlassbezogen statt.

Bei der Prüfung wurde deutlich, dass beim Medizinischen Dienst in der JVA Bremen dem Datenschutz erfreulicherweise ein hoher Stellenwert eingeräumt wird. Kleinere datenschutzrechtliche Mängel wurden umgehend nach der Prüfung behoben.

Folgende Korrekturen mussten seitens des Medizinischen Dienstes vorgenommen werden:

Der Medizinische Dienst bewahrt Patientenakten nunmehr nur noch 20 anstatt 30 Jahre auf. Zwar dürfen behandelnde Ärzte aufgrund des Haftungsrisikos die ärztliche Dokumentation 30 Jahre aufbewahren, für den Medizinischen Dienst der JVA gilt aber die Sonderregelung des § 184 Abs. 3 Satz 1 Strafvollzugsgesetz, wonach

bei der Aufbewahrung von Gesundheitsakten und Krankenblättern eine Frist von 20 Jahren nicht überschritten werden darf.

Ein Formular, mit welchem der Insasse in die Datenerhebung bei externen Ärzten einwilligt, und ein weiteres Formular, die Einwilligung in die Datenverarbeitung bei Substitutionsbehandlungen betreffend, wurden entsprechend meinen datenschutzrechtlichen Anforderungen überarbeitet.

Methadonausgabelisten, die zunächst elektronisch verarbeitet werden, werden gelöscht, wenn die Listen ausgedruckt und geprüft worden sind. Hiermit wurde meine Forderung, dass diese Dateien zu löschen sind, sobald sie nicht mehr erforderlich sind, umgesetzt. Es ist nicht erforderlich, die Daten weiterhin elektronisch zu speichern, wenn sie ohnehin in ausgedruckter Form aufgehoben werden müssen. Zum Zeitpunkt der Prüfung existierte keine Löschfrist für die elektronische Speicherung der Listen.

Die ausgedruckten Methadonlisten werden jetzt auch nur noch drei Jahre – von der letzten Eintragung an gerechnet – aufbewahrt. Hiermit wird den gesetzlichen Anforderungen in § 13 Abs. 3 Satz 1 Betäubungsmittelverschreibungsverordnung Rechnung getragen. Nach Ablauf dieser Frist sind die Daten zu vernichten. Der Medizinische Dienst hat seine Praxis, die Daten 30 Jahre aufzubewahren, geändert und diese damit der Gesetzeslage angepasst.

10.2 Soziale Dienste bei der Justiz

Anfang 2008 wandten sich die Bewährungshelferinnen und -helfer der Sozialen Dienste der Justiz mit diversen datenschutzrechtlichen Fragestellungen an mich. Es ging in erster Linie um die Datenerhebung bei Dritten sowie die Datenübermittlung an Dritte seitens der Bewährungshilfe. Es bestand eine erhebliche Verunsicherung, was aus datenschutzrechtlicher Sicht überhaupt zulässig ist. Die an mich herangetragenen Fragen der Bewährungshilfe mit Beispielsfällen aus der Praxis habe ich zunächst schriftlich beantwortet und dann anschließend die Problematik in einem persönlichen Gespräch erläutert. Kern des Problems ist, dass es sich bei den Bewährungshelferinnen und -helfern um Sozialpädagoginnen und -pädagogen handelt und diese als Berufsgeheimnisträger in § 203 Abs. 1 Nr. 5 Strafgesetzbuch benannt werden. Es besteht die Gefahr des Verstoßes gegen diese Schweigepflicht, wenn sie Informationen über ihre Klienten preisgeben.

Als weiteren Lösungsversuch regte ich eine Erörterung der Rechtsfragen mit dem Senator für Justiz und Verfassung an. Im Rahmen eines Gesprächs, an welchem Vertreter der senatorischen Behörde, der Bewährungshilfe sowie eine Vertreterin aus meiner Dienststelle teilnahmen, konnte jedoch keine abschließende Klärung herbeigeführt werden. Ich schlug daher vor, die Problematik im Rahmen des Arbeitskreises Justiz der Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit meinen Kolleginnen und Kollegen zu diskutieren. Gegebenenfalls könne mit dem Bundesministerium der Justiz Kontakt aufgenommen werden, um den Bewährungshelferinnen und -helfern verbindliche Leitlinien an die Hand zu geben.

10.3 Prüfung der Gerichtsvollzieher

Die Prüfung einiger Gerichtsvollzieher in Bremen und Bremerhaven hatte diverse datenschutzrechtliche Mängel, wie z. B. fehlenden Passwortschutz bei einem Notebook, unzureichende Lagerung von Akten, keine wirksamen Maßnahmen zur Datensicherung sowie die technische Unterstützung von Personen aus dem persönlichem Umfeld, ohne dass diese auf das Datengeheimnis verpflichtet wurden, ergeben. Ich berichtete im 30. Jahresbericht, vgl. dort Ziff. 10.1. Angesichts der festgestellten datenschutzrechtlichen Mängel habe ich die Prüfung zum Anlass genommen, in meinem Haus die Orientierungshilfe „Datenschutz bei Gerichtsvollziehern“ zu erarbeiten. Diese Orientierungshilfe wurde im Juni 2008 mit dem Justizressort und dem Arbeitskreis der Gerichtsvollzieher abgestimmt und an die Amtsgerichtspräsidenten zur Weiterleitung an die Gerichtsvollzieher übersandt. Der Senator für Justiz und Verfassung teilte mir mit, dass die Verteilung der Orientierungshilfe an alle Gerichtsvollzieher erfolgt sei. Die Gerichtvollzieher wurden von den jeweils für sie zuständigen Gerichten aufgefordert, ihre PC bis zum 31. November 2008 entsprechend der Orientierungshilfe zu konfigurieren.

10.4 Schreiben mit Strafvollstreckungserinnerungen geraten außer Kontrolle

Im September wurden mir von einem Journalisten einer Bremer Tageszeitung über 30 fehlgeleitete Schreiben der Staatsanwaltschaft Bremen vorgelegt. Die Zeitung

hatte die Schreiben von einem Informanten erhalten. Es handelte sich hierbei um Mahnungen in Strafvollstreckungssachen. Diese sollten mit einem Anschreiben der Staatsanwaltschaft an die Hausdruckerei der Senatorin für Finanzen per Botenpost geschickt werden, um dort einzeln kuvertiert und frankiert zu werden. Nach Auskunft des Journalisten sollen die Schreiben in einem Umschlag einem Privathaushalt zugestellt worden sein.

Ich habe daraufhin die Staatsanwaltschaft angeschrieben und um umfassende Aufklärung gebeten. Die Staatsanwaltschaft teilte mit, dass derzeit nicht festgestellt werden könne, ob die Fehlleitung der Mahnschreiben auf einem Versehen in der Staatsanwaltschaft beruht oder auf dem abschließenden Transportweg verursacht wurde. Aus der – nicht in der Staatsanwaltschaft erfolgten – Frankierung ergebe sich lediglich, dass der Umschlag von einem unbekannten Zeitpunkt an nicht mehr als Botenpost befördert wurde. Für eine weitere Aufklärung sei die Bekanntgabe des tatsächlichen Empfängers Voraussetzung, welcher von der Zeitung jedoch nicht benannt werden würde.

Auch wenn es sich letztlich wahrscheinlich nicht aufklären lassen wird, wie die Schreiben abhanden kommen konnten, habe ich noch einmal alle Beteiligten zu einem gewissenhafteren Umgang mit derart sensiblen personenbezogenen Daten ermahnt. Die Staatsanwaltschaft hat mir bereits ihrerseits mitgeteilt, dass die mit dem Ausdruck und Weiterleiten von Mahnschreiben an Geldstrafenschuldner befassten Mitarbeiter erneut zu besonderer Sorgfalt angehalten worden sind.

10.5 Bericht aus dem Arbeitskreis Justiz

Der Arbeitskreis Justiz der Konferenz der Datenschutzbeauftragten des Bundes und der Länder tagte im Jahr 2008 einmal. Es wurden u. a. folgende Themen beraten: Einhaltung des Datenschutzes bei Vorgangsbearbeitungssystemen der Staatsanwaltschaften, die Anordnungen von Blutentnahmen durch die Staatsanwaltschaften nach § 81 a Abs. 2 Alt. 2 Strafprozessordnung (StPO), das Gutachten des Max-Planck-Instituts zur „Rechtsverwirklichung der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100 g, 100 h StPO“, DNA-Untersuchungen auf der Grundlage der Einwilligung nach § 81 g StPO zum Zwecke der Speicherung in der DNA-Analysedatei sowie die Übermittlung personenbezogener Daten im Rahmen von Strafverfahren in Europa.

10.6 Vorratsdatenspeicherung

Ein großer Teil der Regelungen zur Vorratsdatenspeicherung ist am 1. Januar 2008 in Kraft getreten (BGBl. I 2007, S. 3198). Das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“, das auf eine Richtlinie der EU (2006/24/EG) zurückgeht, verpflichtet Anbieter von Telekommunikations- und Internetdiensten, umfangreiche Verkehrsdaten der Telekommunikations- und Inter-netnutzung (wie z. B. Rufnummern oder sonstige Kennung des anrufenden und angerufenen Anschlusses, IP-Adressen, Beginn und Ende der Verbindung und Standorte) für ein halbes Jahr auf Vorrat zu speichern. Die gesetzliche Grundlage für die Speicherungspflicht wurde durch das Bundesgesetz geschaffen. Vor Inkrafttreten der Regelung durften die Anbieter nur die zur Abrechnung erforderlichen Verbindungsdaten speichern. Durch die Nutzung von Flatrates konnte die Speicherung gänzlich vermieden werden.

Aus datenschutzrechtlicher Sicht stellen die gesetzlichen Regelungen der Vorratsdatenspeicherung einen unverhältnismäßigen Eingriff in die Grundrechte unbescholtener Bürger dar. Die Datenschutzbeauftragten des Bundes und der Länder haben daher bis zuletzt unermüdlich ihre verfassungsrechtlichen Bedenken geäußert. Leider blieben diese vom Gesetzgeber unberücksichtigt.

Es besteht aber immer noch Hoffnung, dass die gesetzlichen Regelungen außer Kraft gesetzt werden. Zum einen ist eine Klage der Mitgliedstaaten Irland und Tschechien beim Europäischen Gerichtshof (EuGH) anhängig. Sollte der EuGH den Klagen stattgeben, wäre die Richtlinie nichtig.

Zum anderen befasst sich das Bundesverfassungsgericht (BVerfG) derzeit mit Verfassungsbeschwerden von vielen Bürgern und Berufsgruppen. Die Datenschutzbeauftragten des Bundes und der Länder wurden vom Gericht zur Stellungnahme aufgefordert und konnten ihre verfassungsrechtlichen Bedenken erneut vortragen.

Hierbei haben sie insbesondere deutlich gemacht, dass die gesetzlichen Regelungen gegen das Verbot der Vorratssammlung zu unbestimmten oder noch nicht bestimmbaren Zwecken verstoßen und eine unverhältnismäßige Einschränkung des Fernmeldegeheimnisses ermöglichen. Es bleibt zu hoffen, dass das BVerfG im Sinne des Datenschutzes entscheiden wird. Immerhin hat das Gericht im Rahmen einer Eilentscheidung am 11. März 2008 (Az. 1 BvR 256/08) die Anwendung weiter Teile der vom Gesetzgeber verabschiedeten Regelung ausgesetzt. Die für ein halbes Jahr gespeicherten Telekommunikationsverkehrsdaten dürfen vorläufig nur für die Verfolgung besonders schwerer Straftaten nach § 100 a Abs. 2 StPO genutzt werden. Damit ist die Nutzung der Daten für andere im Gesetz genannte Zwecke der Strafverfolgung unzulässig. Das BVerfG beschränkte sich bei seiner vorläufigen Entscheidung jedoch auf die Nutzung der Vorratsdaten, die Verpflichtung der Provider zur Speicherung der Daten auf Vorrat setzt das Gericht demgegenüber nicht vorläufig aus. Hierfür sind vor allem europarechtliche Überlegungen des Gerichts ausschlaggebend.

In einer weiteren Entscheidung am 28. Oktober 2008 (Az. 1 BvR 256/08) hat das BVerfG seine Auffassung erneut bestätigt. Es verlängerte in dieser Entscheidung zum einen die einstweilige Anordnung vom 11. März 2008 um weitere sechs Monate. Gleichzeitig erweiterte es die einstweilige Anordnung vom 11. März 2008 dahingehend, dass die auf Vorrat gespeicherten Daten für die Gefahrenabwehr von Telekommunikationsdiensteanbietern nur unter einschränkenden Bedingungen an die ersuchende Behörde weitergegeben werden dürfen. Eine Übermittlung ist nur zulässig, wenn der Abruf der Daten zur Abwehr einer dringenden Gefahr für Leib, Leben und Freiheit einer Person, für den Bestand und die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr erforderlich ist. Die übermittelten Daten dürfen nur zu den Zwecken verwendet werden, zu denen sie abgerufen wurden.

11. Gesundheit und Krankenversicherung

11.1 Mammographie-Screening

Im Konzept zur Evaluation des Mammographie-Screenings sind umfangreiche Datenübermittlungen zwischen den am Mammographie-Screening beteiligten Stellen (Zentrale Stelle für das Einladungswesen, Screening-Einheiten, Referenzzentrum) und den Krebsregistern vorgesehen. Ich hatte darüber bereits im 30. Jahresbericht (vgl. dort Ziff. 11.1) berichtet. Die Daten sollen unter Verwendung einer in der Zentralen Stelle für jede Teilnehmerin zu bildenden laufenden Nummer (Kommunikationsnummer) zwischen den Stellen übermittelt werden. Von der Screening-Einheit sollen Postleitzahl, Wohnort, Geburtsmonat und -jahr, Screening-Datum und Screening-Ergebnis an das Krebsregister übermittelt werden. Dort sollen die zwischen den Screening-Terminen aufgetretenen Brustkrebserkrankungen (Intervallkarzinome) identifiziert und mit Diagnosedatum und Angaben zum Tumor an das Referenzzentrum Mammographie übermittelt werden. Die Fälle, in denen ein Intervallkarzinom aufgetreten ist, sollen vom Referenzzentrum an die Screening-Einheit gemeldet werden, damit von dort die Screening-Unterlagen der betroffenen Frauen an das Referenzzentrum übermittelt werden können. Eine Einwilligung der Teilnehmerinnen in die Übermittlung ihrer Patientenunterlagen soll nicht eingeholt werden, weil damit gerechnet wird, dass diese in bis zu 40 % der Fälle nicht erteilt werden würde. Eine ausreichende Information der Teilnehmerinnen über die geplanten Datenübermittlungen ist ebenfalls nicht vorgesehen.

Das Konzept ist bereits vom Gemeinsamen Bundesausschuss der Ärzte und Krankenkassen in Form einer Änderung der Krebsfrüherkennungs-Richtlinie beschlossen worden. Dieser Beschluss soll dem Bundesministerium für Gesundheit vorgelegt werden. Eine Verabschiedung ist noch nicht erfolgt. Von den Datenschutzbeauftragten wurde das Konzept unter zahlreichen Gesichtspunkten kritisiert. Die vom Gemeinsamen Bundesausschuss der Ärzte und Krankenkassen beschlossenen Krebsfrüherkennungs-Richtlinien sind keine ausreichende Rechtsgrundlage zur Legitimierung eines derart tiefen Eingriffs in das Recht auf informationelle Selbstbestimmung der Betroffenen. Nach der Wesentlichkeitstheorie des Bundesverfassungsgerichts verpflichten das Rechtsstaatsprinzip und das Demokratieprinzip den Gesetzgeber, die Voraussetzungen für einen Eingriff im grundrechtsempfindlichen Bereich selbst zu regeln. Inhaltlich bestehen starke Bedenken gegen die Verwendung der Kommunikationsnummer als Pseudonym für alle am Abgleich beteiligten

Stellen. Dieses Verfahren sollte aber sicherstellen, dass keine Zusammenführung von Identitäts- und Gesundheitsdaten in den am Abgleich beteiligten Stellen und damit auch der Aufhebung der Anonymität der vom Krebsregister verwendeten Kontrollnummern möglich ist. Die Übermittlung der Screening-Unterlagen (Mammographien und Dokumentation) unter Verwendung der Kommunikationsnummer als Pseudonym von der Screening-Einheit an das Referenzzentrum stellt keine ausreichend sichere Pseudonymisierung dar. Von einem Abgleich in anonymisierter Form, wie in den Krebsfrüherkennungs-Richtlinien beschrieben, kann nicht die Rede sein. Bereits beim von der Screening-Einheit an das Krebsregister zu übermittelnden Datensatz (Kommunikationsnummer, Geburtsmonat und -jahr, PLZ, Wohnort, Screening-Datum und Screening-Ergebnis) kann die Möglichkeit der Identifizierung der Betroffenen nicht ausgeschlossen werden. Ich habe mehrfach darauf hingewiesen, dass die in diesem Konzept vorgesehenen Datenverarbeitungen des Krebsregisters mit dem Bremischen Krebsregistergesetz (BremKRG) unvereinbar sind. In der Vertrauensstelle des BremKRG werden Identitätsdaten dauerhaft gespeichert. Die Aufgaben der Vertrauensstelle sind abschließend festgelegt; die Teilnahme an epidemiologischer Forschung gehört nicht dazu. Eine Übermittlung der Daten ist nur unter den Voraussetzungen des § 7 BremKRG zulässig, der dafür zwingend eine Einwilligung der bzw. des Betroffenen verlangt. Zudem ist die Verarbeitung der von der Screening-Einheit übermittelten Daten in der Registerstelle nach dem BremKRG unzulässig. Deshalb darf auch keine Nutzung (Abgleich mit Krebsregisterdaten, Mortalitätsevaluation) bzw. Übermittlung dieser Daten von der Registerstelle vorgenommen werden. Eine entsprechende Anpassung des BremKRG wird von mir entschieden abgelehnt. Zudem würde mit der Begründung für den Verzicht auf eine Einwilligungserklärung das informationelle Selbstbestimmungsrecht der Betroffenen missachtet. Die Verweigerung der Einwilligung durch Betroffene zeigt doch, wie gravierend der Eingriff in das Recht auf informelle Selbstbestimmung durch die Weitergabe der Patientenunterlagen von den an Brustkrebs erkrankten Frauen empfunden wird. Gerade deshalb darf auf eine Einwilligung hier nicht verzichtet werden. Weiterhin ist die mangelnde Transparenz in Bezug auf die Datenverarbeitung der am Mammographie-Screening beteiligten Stellen gegenüber den Betroffenen Frauen zu kritisieren, denn in dem an die Frauen versandten Informationsblatt werden die vorgesehenen Datennutzungen und -übermittlungen nicht ausreichend beschrieben.

11.2 Elektronische Gesundheitskarte

Der vom Bundesministerium für Gesundheit genannte Termin für den Roll-out der elektronischen Gesundheitskarte (eGK) im zweiten Quartal 2008 konnte erneut nicht eingehalten werden. Nunmehr ist als neuer Termin Ende 2009 angestrebt. Mit einem Roll-out in Bremen kann wohl nicht vor 2010 gerechnet werden. Nach wie vor trifft die eGK bei Ärzten auf heftigen Widerstand; sie wurde mit einer Resolution des 111. Deutschen Ärztetages erneut heftig kritisiert und entschieden abgelehnt.

Im Berichtsjahr traten bei der Testung der Karte in Schleswig-Holstein Probleme auf, weil viele, insbesondere ältere Patienten und solche mit starken gesundheitlichen Einschränkungen, mit der Eingabe der sechsstelligen PIN nicht zurechtkamen. Die beteiligten Ärzte hatten gefordert, die PIN zu deaktivieren, was eine erhebliche Absenkung des Schutzniveaus für alle bedeutet hätte. Diskutiert wurde auch, die PIN in eine einfache Zahlenreihe zu ändern, was aus Datenschutzsicht ebenfalls nicht hingenommen werden kann; zumal gerade bei dieser Patientengruppe hoch sensible Gesundheitsdaten verarbeitet werden. Als Lösung wird favorisiert, dass diese Patienten einem Arzt ihres Vertrauens die PIN offenbaren und dieser insoweit als „Treuhänder“ fungiert. Dieser Arzt soll dann auch zur Weitergabe der PIN an andere behandelnde Ärzte befugt sein. Der Nachteil hierbei ist, dass der Arzt bei Anwesenheit des Patienten in seiner Praxis auch ohne dessen Beteiligung auf die Karte zugreifen könnte.

Getestet wurde über die im Gesetz benannten Funktionen der Karte hinaus auch die Unterbringung einer Organspendeerklärung im Notfalldatensatz der eGK. Neben der fehlenden gesetzlichen Grundlage wurden Bedenken gegen die Realisierung dieser Funktion geäußert, weil der Notfalldatensatz ohne PIN-Eingabe praktisch bei jedem Arztbesuch eingesehen werden kann. Die Einsichtnahme in die Organspendeerklärung ist jedoch nur in einem seltenen Ausnahmefall erforderlich.

Kritisiert wird von den Datenschutzbeauftragten, dass kein übergreifendes Sicherheitskonzept für den gesamten Bereich der Telematikinfrastruktur der eGK, welches auch Krankenhaus-, Apotheken- und Praxisverwaltungssysteme einbezieht, vorliegt oder in Planung ist. Das Bundesministerium für Gesundheit ist aufgefordert worden, hierfür eine Lösung zu finden, da gerade in diesem Bereich erhebliche Sicherheitsrisiken gesehen werden.

Weiterhin ungeklärt ist die Frage der verantwortlichen Stelle, die unter anderem für die Zuordnung der datenschutzrechtlichen Verantwortlichkeit, die Gewährung der Betroffenenrechte sowie die Frage der Aufsichtszuständigkeit von Bedeutung ist. Die einschlägige gesetzliche Regelung des § 67 Abs. 9 Sozialgesetzbuch X wird der Vielzahl der im System der eGK beteiligten Stellen und der Komplexität der Beziehungen nicht gerecht.

11.3 Kindeswohlgesetz

Das Einladungswesen für das Land Bremen zu den Früherkennungsuntersuchungen U 5 bis U 9 durch das Gesundheitsamt Bremen hat zum 1. Dezember 2007 begonnen. Die für die Einführung des zugrunde liegenden technischen Verfahrens erforderliche Untersuchung nach § 7 Abs. 2 Bremisches Datenschutzgesetz (BremDSG), ob und in welchem Umfang mit der Nutzung Gefahren für die Rechte der Betroffenen verbunden sind, ist nicht erfolgt. Auch sind aus der mir zur Verfügung gestellten Kurzbeschreibung die technischen und organisatorischen Maßnahmen zum datenschutzgerechten Einsatz der Software (§ 7 Abs. 3 u. 4 BremDSG) mit Beginn des Verfahrens nicht verfügbar gewesen. Als Übergangslösung wurde eine Access-Datenbank eingesetzt, die keine wirksame Zugangskontrolle (geeignete Maßnahmen zur Identifikation und Authentisierung der Benutzer), Rollendifferenzierung (Definition von benutzerspezifischen Rechten) und Eingabekontrolle (Nachweis der Zugriffe auf die Daten) bereitstellt. Abgesehen von den durch die Art der eingesetzten Datenbank vorhandenen Mängel ist es genereller Standard, auf Datenbanken, die sensible personenbezogene Daten enthalten, ausschließlich (mit Ausnahme der Kennung zu Administrationszwecken) über eine fachspezifische Anwendungssoftware zuzugreifen. Das Gesundheitsamt folgte meiner Argumentation und befindet sich zurzeit in der Anpassung einer durch das Saarland überlassenen Software an die bremischen Anforderungen. Ich gehe davon aus, dass im folgenden Jahr nach Klärung einiger Detailfragen eine fachspezifische Anwendungssoftware mit den erforderlichen technischen datenschutzgerechten Einstellungen zum Einsatz kommen wird.

Bei der Realisierung der Anforderungen an die Datensicherheit habe ich ein hohes Schutzniveau aufgrund der besonderen Sensibilität der beim Gesundheitsamt gespeicherten Daten gefordert. Die besondere Schutzbedürftigkeit der Daten ergibt sich aus dem Verwendungszusammenhang; die Daten über die Teilnahme an Früherkennungsuntersuchungen werden zu dem Zweck gespeichert, Kinder zu identifizieren, deren Wohl gefährdet ist.

Im Rahmen einer datenschutzrechtlichen Prüfung des Umgangs mit Meldungen auf Kindeswohlgefährdungen in einem Sozialzentrum des Amtes für Soziale Dienste (AfSD) habe ich festgestellt, dass im Jugendamt kein festgelegtes Verfahren zum Umgang mit den Meldungen des Gesundheitsamtes existiert. Zum Zeitpunkt der Prüfung im Juli des Berichtsjahres wurde im Sozialzentrum überlegt, die Meldungen ggf. wie Hinweise auf Kindeswohlgefährdungen von Dritten zu behandeln und zunächst durch zwei Mitarbeiter bei der betroffenen Familie einen Hausbesuch durchzuführen. Welche Maßnahmen ergriffen werden sollen bzw. welche rechtlichen Möglichkeiten bestehen, wenn den Mitarbeitern des AfSD der Zutritt zur Wohnung verweigert wird oder beim Hausbesuch keine Auffälligkeiten festgestellt werden, war zu diesem Zeitpunkt völlig ungeklärt. Ebenfalls ungeklärt war der Zweck der ggf. zu ergreifenden Maßnahmen des Jugendamtes in diesen Fällen. Dies hat mich insbesondere deswegen verwundert, da ich bisher davon ausgegangen bin, dass Sinn und Zweck des Kindeswohlgesetzes gerade die Betreuung der Kinder ist, die an den Vorsorgeuntersuchungen nicht teilnehmen. Ich habe die senatorische Dienststelle insoweit zur Stellungnahme aufgefordert. Eine Antwort ist kurz vor Redaktionsschluss eingetroffen, konnte aber noch nicht geprüft werden.

Im August leitete mir die senatorische Dienststelle einen Entwurf zur Änderung des Kindeswohlgesetzes zur Stellungnahme zu. Das Gesetz sollte insoweit ergänzt werden, dass bei Abweichen der Anschrift der gesetzlichen Vertreter von der des

Kindes auch die Anschrift des Kindes übermittelt werden soll. Damit sollten auch fremdplatzierte Kinder korrekt angeschrieben werden können. Dieses Vorhaben begegnete an sich keinen datenschutzrechtlichen Bedenken. Jedoch sollte dafür eine Regelung geschaffen werden, nach der auch die Ärzte in diesen Fällen die Anschrift des Kindes dem Gesundheitsamt mitteilen. Da zu diesem Zeitpunkt nach dem Gesetz bereits mehr Daten von den Ärzten übermittelt werden sollten, als in der Praxis benötigt werden, wandte ich mich gegen diese Erweiterung und forderte stattdessen die Beschränkung dieser Regelung auf die zur Aufgabenerfüllung erforderlichen Daten, nämlich Name, Vorname, Geburtsdatum des Kindes, Datum und Bezeichnung der durchgeführten Untersuchung. Des Weiteren bat ich um die Ergänzung des Gesetzes an die Praxis der Übermittlung insoweit, als vom Meldeamt auch das Ordnungskriterium aus der EMA-Datenbank übermittelt wird. Diese Übermittlung war bislang nicht von einer Rechtsgrundlage gedeckt. Meine Vorschläge wurden von der senatorischen Behörde vollständig übernommen.

11.4 Bericht aus dem Arbeitskreis Gesundheit und Soziales

Der Arbeitskreis Gesundheit und Soziales tagte im März und Oktober des Berichtsjahres. Beraten wurden unter anderem die folgenden Themen: Kindeswohl und Datenschutz, Evaluation des Bundeselterngeld- und Elternzeitgesetzes, oscare-Programm der AOK, Elektronische Gesundheitskarte, Mammographie-Screening, Schutz von Sozialdaten in der ARGE, ELENA sowie einrichtungsübergreifende elektronische Fallakten.

12. Arbeit und Soziales

12.1 Prüfung im Sozialzentrum Gröpelingen/Walle

Im Juli des Berichtsjahres habe ich die seitens des Sozialzentrums Gröpelingen/Walle des Amtes für Soziale Dienste erfolgende Datenverarbeitung im Zusammenhang mit Hinweisen auf Kindeswohlgefährdung geprüft. Im Sozialzentrum Gröpelingen/Walle wird dem Datenschutz erfreulicherweise eine hohe Bedeutung für die Arbeit mit den Betroffenen beigemessen. Soweit möglich wird versucht, hinsichtlich der im Rahmen der Aufgabenerfüllung notwendigen Datenübermittlungen den Betroffenen gegenüber Transparenz herzustellen und die Datenübermittlungen im Einvernehmen mit dem Betroffenen vorzunehmen.

Das Sozialzentrum erhält Hinweise auf Kindeswohlgefährdung von der Polizei, der BAgIS, Schulen, Kindergärten, Bürgern, Kinderärzten und vereinzelt auch von Beratungsstellen. Dabei fällt auf, dass in vielen Fällen die hauptsächliche Motivation der meldenden Stellen die eigene Entlastung ist. Oft wird vorschnell gemeldet, ohne dass im Einzelfall begründete Hinweise auf eine Kindeswohlgefährdung vorhanden sind. Das ist vor allem bei der BAgIS zu beobachten, die zum Teil bereits Meldungen macht, wenn Leistungen gekürzt werden oder kein Folgeantrag gestellt wird. Im Sozialzentrum besteht ein Interesse daran, dass die meldende Stelle den Betroffenen gegenüber Transparenz herstellt. Bevorzugt werde ein Erstkontakt mit dem Jugendamt in der meldenden Einrichtung mit Einwilligung der Betroffenen. Dieses Verfahren funktioniert zum Teil in Kindergärten und Schulen sehr gut. Von vielen Stellen werden jedoch heimliche Meldungen bevorzugt, weil die Auseinandersetzung mit dem Betroffenen gescheut wird, oder es wird, insbesondere von Ärzten, auf das Vertrauensverhältnis zum Betroffenen verwiesen und darauf, dass befürchtet werde, dass der Betroffene bei Kenntnis von der Meldung den Kontakt abbrechen könnte.

Grundsätzlich wird jedem Hinweis auf eine mögliche Kindeswohlgefährdung nachgegangen. Bei Eingang einer Meldung wird zunächst geprüft, ob die betroffene Familie im Sozialzentrum bekannt ist. In der Regel statten noch am gleichen oder am auf die Meldung folgenden Tag Beschäftigte der betroffenen Familie einen Hausbesuch ab. In den Fällen, in denen sich die Meldung auf eine mögliche Kindeswohlgefährdung nicht bestätigt, entweder weil eine absichtliche Falschmeldung vorliegt oder weil bei einem Hausbesuch keine Anhaltspunkte für eine Kindeswohlgefährdung festgestellt werden, wird die Meldung in einem Ordner für unbestätigte Hinweise gesondert abgeheftet. Eine Löschfrist für die Meldungen in diesem Ordner gab es zum Zeitpunkt der Prüfung nicht.

Bei Nachfragen der Meldenden nach den Ergebnissen, dem Verfahrensstand, etc. in der Sache wird vom Sozialzentrum grundsätzlich keine Auskunft erteilt. Kinder-

ärzten wird mitgeteilt, dass sich um die Angelegenheit gekümmert werde, oder eventuell, dass das Kind aus der Familie genommen wurde und daher nicht wieder bei diesem Arzt erscheinen wird. Soweit von Eltern des betroffenen Kindes für dieses eine Schweigepflichtentbindungserklärung abgegeben wird, werden im Einzelfall auch mehr Daten mit den Ärzten ausgetauscht.

Ich habe das Sozialzentrum auf die Möglichkeit der Datenübermittlung aufgrund einer Einwilligungserklärung hingewiesen, wobei dem Betroffenen Zweck und Umfang der Datenverarbeitung bekannt sein muss, d. h., er muss wissen, wer welche Daten von ihm aus welchem Grund speichert und ggf. an wen welche Daten zu welchem Zweck übermittelt werden. Zudem müssen ihm die Freiwilligkeit, die Konsequenzen der Nichterteilung der Einwilligung und die Möglichkeit zum Widerruf für die Zukunft bekannt gemacht werden. Grundsätzlich ist eine Einwilligungserklärung schriftlich einzuholen. Ich habe es begrüßt, dass vonseiten des Sozialzentrums an die meldenden Stellen kommuniziert wird, dass ein transparentes Verfahren, in dem der Betroffene von der meldenden Stelle über die Tatsache der Meldung im Vorhinein informiert wird, bevorzugt wird. Aus datenschutzrechtlicher Sicht ist ein transparentes Verfahren zur Wahrung der schutzwürdigen Belange des Betroffenen grundsätzlich erforderlich, es sei denn, dass im Ausnahmefall besondere Gründe für die Geheimhaltung bestehen. Weiterhin habe ich darauf hingewiesen, dass für die Meldungen, bei denen sich nach Prüfung der Verdacht auf eine Kindeswohlgefährdung nicht bestätigt hat, eine Löschfrist festgelegt werden muss. Ich habe darauf hingewiesen, dass Ersuchen von Dritten nach Auskunft über den aktuellen Stand in den Verfahren des Sozialzentrums nicht nachgekommen werden darf. Das Sozialzentrum will diese Punkte umsetzen.

12.2 BAgIS und ARGE Job-Center Bremerhaven

Meine Hoffnungen auf eine weitere Verbesserung der Zusammenarbeit mit der BAgIS haben sich für das Berichtsjahr 2008 leider nicht erfüllt. Die Anzahl der Bürgereingaben ist überproportional angestiegen. Die dabei aufseiten der ARGEn festgestellten Verstöße gegen Datenschutzvorschriften betrafen überwiegend immer die gleichen Sachverhalte, deren Unzulässigkeit in den einzelnen Geschäftsstellen aufgrund meiner Interventionen eigentlich längst bekannt sein müssten. In der BAgIS Süd musste ich sogar vonseiten der Geschäftsstellenleitung einen erheblichen Widerstand gegen meine Aufsichtstätigkeit erfahren, der sich darin äußerte, dass zeitweise die Beantwortung meiner Fragen verweigert wurde und meine Forderungen nicht umgesetzt worden sind. Dieser Konflikt konnte schließlich durch die Einschaltung des Geschäftsführers aufgelöst werden.

Datenschutzverstöße wurden im Berichtsjahr unter anderem häufig festgestellt in Bezug auf die Anforderung und Anfertigung von Kopien von Kontoauszügen und Personalausweisen, mangelnde Vertraulichkeit in den Räumen der Geschäftsstellen gegenüber anderen Kunden, unbefugte Datenerhebungen bei Dritten (z. B. der swb und privaten Maßnahmeträgern), unbefugte Datenübermittlungen an Dritte (z. B. große Absenderstempel auf Briefen an Hilfeempfänger, Einsatz von privaten Sicherheitsdiensten in den Beratungszimmern und Platzierung von personenbezogenen Bewerberprofilen im Internet), Erhebung und Speicherung von für die Aufgabenerfüllung nicht erforderlicher Daten (z. B. Aufforderung zum Ausfüllen eines Gesundheitsfragebogens und Speicherung eines Diebstahlsverdachts des ehemaligen Arbeitgebers), Androhung von Sanktionen bei Verweigerung der Erteilung von Schweigepflichtentbindungserklärungen.

12.3 Elektronischer Entgeltnachweis (ELENA)

Mit dem Projekt ELENA soll eine zentrale Speicherung von Einkommensdaten der gesamten deutschen abhängig Beschäftigten, Beamten, Richter und Soldaten zum Zweck der elektronischen Ausstellung von Einkommensnachweisen bei der Beantragung von Sozialleistungen erfolgen. Ich hatte darüber bereits im 27. Jahresbericht (vgl. dort Ziff. 1.10) und im 28. Jahresbericht (vgl. dort Ziff. 12.3) berichtet. Ein entsprechender Gesetzesentwurf ist im Juni des Berichtsjahres von der Bundesregierung beschlossen worden. Mit der Speicherung der Daten für den Bereich der sozialen Leistungen der Bundesagentur für Arbeit, der Elterngeld- und Wohngeldstellen soll im Jahr 2012 begonnen werden. Weitere Leistungen sollen später hinzukommen. Die Datenschutzbeauftragten hatten seit langem kritisiert, dass es sich dabei um eine unzulässige Vorratsdatenspeicherung von sensiblen Daten handelt, die bei einem großen Teil der Betroffenen für die festgelegten Zwecke nicht benö-

tigt wird. Vonseiten der Datenschutzbeauftragten wurde zudem eine Verschlüsselung der gespeicherten Datensätze gefordert, die jedoch nicht umgesetzt worden ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dazu zuletzt im November 2008 in einer Entschließung Zweifel an der Verfassungsmäßigkeit geäußert und weitere technische und organisatorische Maßnahmen im Hinblick auf die Berücksichtigung datenschutzrechtlicher Grundsätze im Verfahren, ein differenziertes Löschkonzept, die Ver- und Entschlüsselung der Daten, Authentisierungsverfahren der abrufenden Stellen und eine unabhängige Zertifizierung gefordert (vgl. Ziff. 20.16 dieses Berichts).

12.4 Onlinezugriff der Sozialbehörden auf Meldedaten

Im April des Berichtsjahres wandte sich die Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales an das Stadtamt, um dort für die senatorische Dienststelle und das Amt für Soziale Dienste Onlinezugriffe auf das Melderegister einrichten zu lassen. Als Begründung wurde angeführt, dass die Daten dort für die Aufgabenerfüllung benötigt würden und es zur Erleichterung und Beschleunigung der Vorgangsbearbeitung führen würde. Der Zugriff sollte ohne Vorliegen einer Rechtsgrundlage in der Meldedatenübermittlungsverordnung (MeldDÜV) geschaffen werden. Ich wies die senatorische Behörde darauf hin, dass diese allgemeinen Angaben zur Begründung der Erforderlichkeit für einen Onlinezugriff auf das Melderegister nicht ausreichen, sondern dass es der Begründung der Erforderlichkeit und Angemessenheit für jede einzelne abrufende Stelle in Bezug auf ihre Aufgabenerfüllung bedarf. Die Voraussetzungen seien grundsätzlich nur bei Massenverfahren oder bei besonderer Eilbedürftigkeit erfüllt und es bedürfe insoweit auch einer Rechtsgrundlage in der MeldDÜV. Die Sozialsenatorin war zunächst nicht bereit, die von mir geforderten entsprechenden Fallzahlen und Daten bereitzustellen, die für die Prüfung der Voraussetzungen für die Einrichtung des Onlineabrufs für jede einzelne Stelle erforderlich sind. Ich bat insoweit nochmals um Konkretisierung, die jedoch nicht erfolgte. Auf Wunsch der senatorischen Dienststelle erläuterte ich meine Anforderungen im August erneut in einem persönlichen Gespräch, woraufhin mir die Bereitstellung der entsprechenden Informationen zugesagt wurde. Daraufhin wurde mir Ende Oktober eine Tabelle mit einer Auflistung von zehn Arbeitsbereichen übermittelt, deren Aufgaben im Zusammenhang mit der Anzahl der notwendigen Meldeamtsanfragen pauschal stichwortartig aufgelistet waren, und es wurde eine kurzfristige Zustimmung vor Weihnachten für vier der genannten Bereiche erbeten. Dies musste ich jedoch vorläufig zurückweisen, da weder eine Rechtsverordnung erlassen worden ist noch die vom Gesetz vorgesehene Verfahrensbeschreibung vorliegt und auch keine Angemessenheitsprüfung durchgeführt bzw. dokumentiert worden ist.

13. Bildung und Wissenschaft

13.1 Videoüberwachung in Schulen

Kurz vor den Sommerferien 2008 hat mich der Medienausschuss der Bremischen Bürgerschaft (Landtag) gebeten zu untersuchen, ob der Einsatz von Videoüberwachungen in Schulen datenschutzgerecht erfolge. Dazu habe ich die Senatorin für Bildung und Wissenschaft und das Schulamt Bremerhaven gebeten festzustellen, in welchen Schulen jeweils welcher Bereich videoüberwacht wird und ob jeweils ein Datenschutzkonzept erstellt wurde. Nach Mitteilung der beiden Schulverwaltungen wird an ca. 20 Schulen Videoüberwachung eingesetzt. In praktisch allen Fällen erfolgte keine Beteiligung des behördlichen Datenschutzbeauftragten. Die behördlichen Datenschutzbeauftragten haben mir auf Anfrage mitgeteilt, im Rahmen einer nachträglichen Beteiligung auf eine Anpassung an die Vorgaben des § 20 b Bremisches Datenschutzgesetz (BremDSG) hinzuwirken.

Außerdem lag in den meisten Fällen kein angemessenes Datenschutzkonzept vor; insbesondere hat häufig die gesetzlich vorgeschriebene Anordnung der Leitung der jeweiligen Schule, die den Zweck, die räumliche Ausdehnung und die Dauer der Videoüberwachung dokumentiert, gefehlt.

Bisher bin ich von Lehrern nur auf die Videoüberwachung im Eingangsbereich des Alten Gymnasiums in Bremen hingewiesen worden. Den Schülerinnen und Schülern sowie Lehrkräften sei dies nicht bekannt gewesen, auch befänden sich dort keine entsprechenden Hinweise. Die Schulleiterin hat auf meine Anfrage erklärt,

die Videoüberwachung sei wohl im Jahre 2000 durch ihren Vorgänger veranlasst worden, weil der Hausmeister mehrfach überfallen worden sei. Hinweisschilder seien nicht angebracht worden, weil nicht klar gewesen sei, ob dies erlaubt sei.

Die Schulleitung hat daraufhin eine entsprechende dienstliche Anordnung erlassen sowie eine Verfahrensbeschreibung erstellt, die auch die vorgenannten Anforderungen erfüllt. Jeder kann die Anordnung im Sekretariat einsehen.

Nachdem seit 2003 die Vorschrift des § 20 b BremDSG besteht, habe ich keine generellen Bedenken gegen die Videoüberwachung der Eingangsbereiche von Schulen, weil damit insbesondere der Hausmeister geschützt und Einbrüchen oder Vandalismus vorgebeugt wird. Allerdings müssen Vorkehrungen zur Wahrung schutzwürdiger Belange der Betroffenen (Schülerinnen und Schüler, Lehrkräfte, sonstiges Personal, Eltern und Besucher) getroffen werden. Dazu gehörten insbesondere, dass die Videoüberwachung nur außerhalb der Ganztagsschulzeiten in der Zeit von 16.00 Uhr nachmittags bis 7.00 Uhr am nächsten Morgen stattfindet und entsprechende Hinweise angebracht werden.

13.2 Übermittlung von Erstklässlerdaten an Bremer Tageszeitung

Das Bildungsressort hatte zusammen mit anderen Organisationen, wie Zentralelternbeirat und Verkehrswacht, einen sog. Elternbrief an die Erstklässler entworfen, der, ergänzt um Werbung und Informationen einer Bremer Tageszeitung, von dieser kostenlos an die Eltern der Einzuschulenden versandt wurde. Die zugehörigen Adressdaten wurden vom Bildungsressort unverschlüsselt per E-Mail der Bremer Tageszeitung übermittelt. Eine schriftliche Vereinbarung über den Umgang mit den zur Verfügung gestellten Daten wurde nicht geschlossen, vielmehr wurde alles telefonisch erledigt. Die Sache, die einem guten Zweck dienen sollte, wurde ohne jeden Gedanken an den Datenschutz betrieben. Unabhängig davon, ob und bejahenden Falles unter welchen Voraussetzungen im Einzelnen eine solche Adressmitteilung hätte stattfinden dürfen, wurde nicht einmal das kleine Einmaleins der Datensicherheit beachtet. Auf meine Nachfrage hat das Ressort erklärt, dies werde bereits seit mehreren Jahren so gehandhabt, allerdings bestünden nunmehr Zweifel, ob die Übermittlung zulässig sei. Mit der Bremer Tageszeitung sei vereinbart worden, die Daten nur für den Versand des Elternbriefes zu verwenden und sie anschließend zu löschen. Die Daten seien im Anschluss an den Versand der Elternbriefe vernichtet worden.

Das Ressort erkennt an, dass bei der Durchführung der Aktion dem Datenschutz nicht in ausreichendem Maße Rechnung getragen wurde und hat, nachdem ich auf ein einschlägiges Urteil des Bundesgerichtshofs (BGH) vom 18. Oktober 2001 (Az. IZR 193/99) hingewiesen habe, das allerdings wettbewerbsrechtliche Fragen in den Vordergrund stellt, erklärt, es werde zunächst prüfen, ob zukünftig ganz auf diese Aktion verzichtet werden müsse, anderenfalls wolle es bereits bei der Planung den Datenschutz berücksichtigen.

13.3 Bericht aus der Arbeitsgruppe Schule/Bildung

Die 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Oktober 2007 die Einrichtung einer Arbeitsgruppe Schule/Bildung beschlossen. Konkreter Auftrag der AG ist es, angesichts der Entwicklungen in der Informationsgesellschaft, namentlich des Internets, das Datenschutzbewusstsein von Schülerinnen und Schülern zu verbessern bzw. erst zu schaffen. Ich beteilige mich an der Arbeitsgruppe. Erstes Ergebnis ihrer Arbeit ist u. a. die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder verabschiedete Entschließung „Medienkompetenz und Datenschutzbewusstsein in der jungen Online-Generation“.

14. Umwelt, Bau, Verkehr und Europa

14.1 Erhebung von Gesundheitsdaten bei Ausnahmen vom Fahrverbot in einer Umweltzone

Der Senator für Umwelt, Bau, Verkehr und Europa hat mich im Rahmen der Beteiligung der Öffentlichkeit und Träger öffentlicher Belange zum Vorhaben, in der Stadt Bremen eine Umweltzone einzurichten, um Stellungnahme gebeten. Nach Ziffer 2.1 Buchstabe f des Leitfadens zur einheitlichen Handhabung der Genehmigung von Einzelausnahmen zum Fahrverbot in einer Umweltzone Bremens sind

vom Fahrverbot generell Fahrzeuge ausgenommen, mit denen Personen fahren oder gefahren werden, die im besonderen Maße behindert, hilflos oder blind sind.

Ich habe der senatorischen Dienststelle dargelegt, dass es für die Erteilung einer Einzelausnahme für Personen, denen gesundheitsbedingt die Nutzung öffentlicher Verkehrsmittel nicht möglich ist, ausreiche, sich ein ärztliches Attest vorlegen zu lassen, das lediglich die „eingeschränkte Mobilität" bescheinigt. Beispielhaft habe ich mich dabei auf die Bescheinigung von „Dienst- oder Arbeitsunfähigkeit" bezogen, die nicht die Art der Erkrankung, sondern nur die Folge, nämlich die Tatsache der Arbeitsunfähigkeit bescheinigt. Mir ist zugesagt worden, so zu verfahren.

14.2 Die aktuelle Verkehrslage auf Bremer Autobahnen im Internet

Verursacht durch das Aufstellen von Hinweisschildern auf der A 1 und der A 27 zur Videoüberwachung wurde ich im Sommer des Jahres mehrfach von besorgten Bürgern, aber auch von Abgeordneten im Medienausschuss (Ausschuss für Informations- und Kommunikationstechnologie und Medienangelegenheiten) angesprochen, ob denn das, was dort gemacht werde, datenschutzrechtlich unbedenklich sei. Ein Bürger sagte z. B. am Telefon, er könne ja schließlich auf der Autobahn nicht umdrehen, wenn er das Hinweisschild zur Videoüberwachung gelesen habe. Auch die Veröffentlichung von den Webcam-Bildern im Internet hat eine Reihe von Reaktionen hervorgerufen.

Ich habe daraufhin eine technische Untersuchung der Internetveröffentlichung in meinem Hause in Auftrag gegeben. Diese Untersuchung hat ergeben, dass mit herkömmlich verfügbarer Software weder die Gesichter der in den Fahrzeugen befindlichen Personen noch die Kfz-Kennzeichen erkenn- und lesbar gemacht werden können. Dies gilt auch für die beim Bundeskriminalamt (BKA) vorhandene Spezialsoftware, die auch aus schlecht aufgelösten Bildern noch das Autokennzeichen ermitteln kann, wie mir der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit auf Nachfrage versicherte.

Es hätte jedoch die bei der Bremer Verkehrsmanagementzentrale (VMZ) auflaufende Bildqualität eine personenbeziehbare Darstellung der Bilder ermöglichen können. In einem weiteren Schritt habe ich daher die tatsächliche Bildqualität bei der VMZ untersucht. Die Prüfung ergab keine Abweichung. Die VMZ empfängt nur die auch im Internet veröffentlichte Bildqualität (Pixelzahl), auch für die VMZ gilt daher das oben genannte Ergebnis.

Allerdings wurde von Mitgliedern der Verkehrsdeputation moniert, dass bei Lastwagen, die mit großen Buchstaben beschriftet seien, Rückschlüsse gezogen werden könnten. Das Aufzeichnungsraster wurde daher von der VMZ noch weiter vergröbert, sodass auch dies nicht mehr erkennbar ist.

Ich bin daher zu dem Ergebnis gekommen, dass mit den Videobildern von der A 1 und der A 27 keine personenbeziehbaren Daten in das Internet eingestellt werden und es nach Datenschutzrecht keinen Anlass gab, den Vorgang zu beanstanden. Dieses Ergebnis habe ich auch dem Medienausschuss wie in der Verkehrsdeputation berichtet.

Allerdings hatte der Vorgang durch die Hinweisschilder noch eine weitere Komponente. Die Bürgerinnen und Bürger, die im Vorbeifahren die Hinweisschilder auf die Videoüberwachung lesen, dachten natürlich, sie würden persönlich mit dem jeweiligen Kennzeichen erfasst. Gerade die jüngsten Debatten über die automatische Kennzeichenerfassung („automatisierter polizeilicher Kennzeichenscan") begünstigten diese Annahme.

Während auf einer der Sitzungen der Bremischen Bürgerschaft erst kurz zuvor beschlossen wurde, die entsprechende Regelung aus dem Polizeigesetz (BremPolG) zu streichen, entstand an der Autobahn für die Bürgerinnen und Bürger der Eindruck, Bremen habe nunmehr eine solche Technik installiert. Diese falsche Annahme wurde dadurch noch verstärkt, dass bei personenbeziehbarer Bilderfassung die Datenschutzgesetze entsprechende Hinweisschilder notwendig machen, wie z. B. bei der Videoüberwachung auf dem Bahnhofsvorplatz. Da die Hinweisschilder rechtlich nicht geboten waren und zu den genannten Irritationen bei den Vorbeifahrenden führten, hat die VMZ die Hinweisschilder wieder entfernt.

14.3 Datenweitergabe an Dritte durch die Architektenkammer

Ich bin darüber informiert worden, die Architektenkammer verwende eine Einwilligungsklausel, in der ohne Angabe der jeweiligen Zwecke die Datenempfänger

nur beispielhaft (z. B. Deutsches Architektenblatt, Versorgungswerk der Architektenkammer, Deutsche Krankenversicherung, Veröffentlichung im Internet) benannt würden.

Ich habe die Architektenkammer darauf hingewiesen, dass diese Klausel nicht die Anforderungen nach § 3 Abs. 3 Bremisches Datenschutzgesetz (BremDSG) erfüllt, wonach der Betroffene in geeigneter Weise über den Zweck der beabsichtigten Datenübermittlung aufzuklären ist. Zudem lässt diese Klausel keine Differenzierung hinsichtlich der Empfänger zu, sodass eine Einwilligung in die Datenübermittlung nur an alle Empfänger möglich ist. Außerdem sind die Empfänger in der Klammer nur beispielhaft benannt, sodass für den Betroffenen nicht erkennbar ist, an welche sonstigen Stellen seine Daten übermittelt werden sollen.

Auf meinen Vorschlag hin hat die Architektenkammer eine differenzierte Einwilligungserklärung entwickelt, die die gesetzlichen Anforderungen erfüllt.

15. Finanzen

15.1 Xpider

Die Internetsuchmaschine Xpider (extended spider) ist ein Webcrawler, der im Bereich der Steuerfahndung eingesetzt wird. Xpider dient der Kontrolle des gewerbsmäßigen Handels im Internet, wozu auch Internetauktionshäuser wie Ebay zählen. Das Teilprojekt des Kontrollmitteilungsverfahrens Xpider wird vom Bundeszentralamt für Steuern (BZSt) betrieben. Die Ermächtigung des BZSt ergibt sich aus § 5 Abs. 1 Nr. 17 Finanzverwaltungsgesetz.

Xpider sammelt Daten zu steuerlich nicht registrierten unternehmerischen Aktivitäten, die dann an die Finanzbehörden der Bundesländer weitergegeben werden. Mit Hilfe des Xpidersystems können Verkaufsplattformen durchforstet, Querverbindungen zwischen An- und Verkäufen hergestellt und Abgleiche mit Handelsregistern und anderen Datenbanken vorgenommen werden.

Als problematisch wird die Übermittlung von unzähligen Daten durch Xpider gesehen, deren Erfolgsquote bisher nur im Promillebereich lag. Der Bundesrechnungshof berichtete, dass der Einsatz von Xpider wirkungslos sei und nur Kosten verursache. Diesen Bericht des Bundesrechnungshofs und die BT-Drs. 16/7978 vom 6. Februar 2008 „Auf den Spuren von Internet-Verkäufern“ habe ich zum Anlass genommen, an die Finanzverwaltung in Bremen im Mai 2008 heranzutreten. Im Juli 2008 berichtete mir die Finanzverwaltung über das Verfahren. Die Ergebnisse von Xpider werden quartalsweise per optischem Datenträger an die Finanzverwaltung gesendet. Ich habe in einem Gespräch mit der Finanzverwaltung über die gebräuchlichen Datenschutzanforderungen, wie Aufbewahrungs- und Löschfristen von für die Finanzverwaltung erforderlichen Daten, informiert. Unbrauchbare Daten sind nicht erforderlich und daher sofort zu löschen. Des Weiteren machte ich auf mein Merkblatt zum Vernichten von Daten, wie zum Beispiel bei optischen Datenträgern, aufmerksam, welches auch auf meiner Homepage unter der Rubrik „Hilfestellung“ zu finden ist. Darüber hinaus interessiert mich, wie erfolgreich der Einsatz von Xpider in Bremen ist. Derzeit liegen mir noch keine Zahlen vor, die es mir ermöglichen, die Qualität zu beurteilen.

15.2 Steueridentifikationsnummer

Die Einführung der bundeseinheitlichen Steueridentifikationsnummer (vgl. 30. JB, Ziff. 15.1) führte bundesweit zu Datenpannen, insbesondere weil keine aktuellen Daten vom Bundeszentralamt für Steuern (BZSt) zur Adressierung der Briefe verwendet wurden. Bundesweit wurden Presseberichten zufolge ca. eine Million Briefe falsch adressiert. Eine massive Gefährdung der Daten geht trotz Briefgeheimnisses damit einher. Viele andere waren inhaltlich falsch. Im Bundesland Bremen beliefen sich die fehlerbehafteten Schreiben auf ca. 7000. Insgesamt muss also ein schlampiger Umgang mit Steuerdaten seitens des BZSt konstatiert werden. Das BZSt hat die Software überarbeiten lassen, und die Meldebehörden haben die Daten aktualisiert.

15.3 Auskunftsanspruch in der Finanzverwaltung

In seinem Beschluss vom 10. März 2008 (Az. 1 BvR 2388/03) bestätigte das Bundesverfassungsgericht (BVerfG) den Auskunftsanspruch der Bürgerinnen und Bür-

ger gegenüber der Finanzbehörde gemäß § 19 BDSG entgegen der Rechtsauffassung des Bundes und der Länder, die bisher vertreten hatten, dass das Bundesdatenschutzgesetz nicht anwendbar sei. Diese höchstrichterliche Entscheidung ist richtungsweisend für den Bereich der Finanzverwaltung. Sie stärkt das Informationsrecht der Bürgerinnen und Bürger und trägt dem Gedanken von Transparenz Rechnung. Für ein finanzbehördliches Ermessen bei der Entscheidung über die Auskunftserteilung ist verfassungsrechtlich kein Raum. Das BVerfG statuiert, dass „eine Auskunft nur dann unterbleiben darf, wenn das Interesse an der ordnungsgemäßen Aufgabenerfüllung dem Informationsinteresse des Betroffenen vorgeht."

15.4 Bericht aus dem Arbeitskreis Steuerverwaltung

Der Arbeitskreis Steuerverwaltung der Konferenz der Datenschutzbeauftragten des Bundes und der Bundesländer beschäftigte sich im April 2008 mit Themen wie der Vergabe von Steueridentifikationsnummern (vgl., Ziff. 15.2), Xpider (vgl., Ziff. 15.1), der Änderung der Kirchensteuergesetze sowie VoIP (Voice over IP als internetbasierte Sprachtelefonie) in der Finanzverwaltung. Daneben wurde die Ausgestaltung eines Auskunftsanspruchs in der Abgabenordnung (AO) angesichts der neuen Entscheidung des Bundesverfassungsgerichts (BVerfG) zu den Domizilgesellschaften vom 10. März 2008 (vgl. Ziff. 15.3) diskutiert.

Im Lichte dieser neuen Entscheidung des BVerfG befasste sich der Arbeitskreis mit der Entscheidung des BVerfG vom 13. Juni 2007 (BvR 1550/03) zur Kontodatenabfrage (vgl. 30. JB, Ziff. 15.3). Der § 88 a AO wird in der neuen Entscheidung des BVerfG verfassungsgemäß als gesetzliche Grundlage für die Speicherung von Informationen in einer Datensammlung angesehen. Die Beurteilung bezieht sich zunächst auf die Sammlung von Daten über im Inland ansässige Firmen des Instituts für Auslandsbeziehungen. Eine grundsätzliche Auseinandersetzung mit dieser Norm durch das BVerfG, insbesondere in Bezug auf Vorratsdatensammlungen (wie zum Beispiel ZAUBER) und nach den Maßstäben der bisherigen Entscheidung des Bundesverfassungsgerichts zur Kontendatenabfrage im Jahre 2007, ist leider nicht erfolgt. So wird zum Beispiel die Normenklarheit der Regelung in der neuen Entscheidung des BVerfG (Rn. 85, 86) nur in einem Satz knapp erwähnt. § 88 a Abgabenordnung (AO) kann daher grundsätzlich nicht als Rechtsgrundlage für Vorratsdatensammlungen ausreichen.

16. Bremerhaven

16.1 Themen aus Bremerhaven

An dieser Stelle werden alle Ziffern dieses Berichts aufgeführt, die sich mit Themen aus Bremerhaven beschäftigen. Sie finden sich unter Ziff. 7.1 (Ergebnisse der Beratungen des 30. Jahresberichts), Ziff. 7.3 (Abschaffung der automatischen Kfz-Kennzeichenerfassung), Ziff. 9.1 (Unberechtigter Zugriff auf Online-Melderegister war möglich), Ziff. 9.2 (Übermittlung von Meldedaten an Adresshändler), Ziff. 9.12 (Eingaben im Bereich der Polizei Bremen und Bremerhaven), Ziff. 9.20 (Unfalldatenschreiber bei der Feuerwehr), Ziff. 10.3 (Prüfung der Gerichtsvollzieher), Ziff. 12.2 (BAgIS und ARGE Job-Center Bremerhaven), Ziff. 13.1 (Videoüberwachung in Schulen), Ziff. 16.2 (Weitergabe von Diagnosedaten bei Dienstunfall einer Lehrerin), Ziff. 16.3 (Speicherung falscher Daten zur Staatsangehörigkeit im Melderegister), Ziff. 17.3 (2. Europäischer Datenschutztag), Ziff. 18.2 (Digitale Straßenansichten), Ziff. 18.6.1 (Datenschutzskandal bei einem Callcenter der Telekom), Ziff. 18.7.3 (Videoüberwachung in einem Einkaufszentrum) und Ziff. 18.13.4 (Videoüberwachung von Beschäftigten).

16.2 Weitergabe von Diagnosedaten bei Dienstunfall einer Lehrerin

Im März des Berichtsjahres wandte sich eine Lehrerin an mich und teilte mit, dass sie einen Antrag auf Anerkenntnis eines Dienstunfalls gestellt habe. Der Schriftverkehr in Bezug auf die Anerkenntnis, der Diagnosedaten und weitere Einzelheiten in Bezug auf den Gesundheitszustand der Betroffenen enthielt, wurde ihr vom Personalamt des Magistrats der Stadt Bremerhaven auf dem Dienstweg zugeleitet. Dadurch erhielten auch das Schulamt und der Schulleiter Kenntnis von den Gesundheitsdaten. Auf meine Aufforderung zur Stellungnahme teilte das Personalamt mit, dass Angaben zum Dienstunfall dem Vorgesetzten von der Betroffenen ohnehin zur Kenntnis gegeben werden müssten. Deshalb sei auch die Diagnose

dort bereits bekannt. Die Versendung der Bescheide auf dem Dienstweg sei erforderlich, um den Schulleiter und das Schulamt über die Anerkenntnis als Dienstunfall zu informieren, diese Information würde dort für die Einsatzplanung in Bezug auf die Betroffene benötigt. Einen Verstoß gegen datenschutzrechtliche Bestimmungen könne es nicht erkennen. Ich teilte dem Personalamt mit, dass nach dem Grundsatz der Vertraulichkeit von Personalaktendaten eine Weiterleitung von Diagnosedaten zu den genannten Zwecken unzulässig ist und forderte dazu auf, davon zukünftig abzusehen. Die Kenntnis der in den Bescheiden enthaltenen Diagnose- und weiteren Gesundheitsdaten ist für die Erfüllung der Aufgaben des Schulamtes und des Schulleiters nicht erforderlich. Zum einen wird sich nicht in allen Fällen nach einem Dienstunfall die Notwendigkeit ergeben, die Lehrkraft zeitweise oder dauerhaft anders als bisher einzusetzen. Zum anderen gehört es weder zu den Aufgaben des Schulamtes oder des Schulleiters noch haben diese die notwendige fachliche Qualifikation, um die gesundheitliche Eignung des Bediensteten für seine ausgeübten Tätigkeiten festzustellen. Eine entsprechende Feststellung kann nur durch einen Arzt getroffen werden. Deshalb kann natürlich auch nicht davon ausgegangen werden, dass die später vom Arzt festgestellten Diagnosen dem Schulleiter aufgrund der Kenntnis vom Dienstunfall bereits bekannt sind. Vom Personalamt bekam ich zur Antwort, dass meine Rechtsauffassung dort nicht geteilt würde und dass auch zukünftig bei Dienstunfällen entsprechend verfahren würde. Ich wandte mich daher an den Magistrat der Stadt Bremerhaven. Ende November wurde mir vom Personalamt mitgeteilt, dass meine Vorgaben dort nun akzeptiert und dass man sich zukünftig daran halten werde. Das Personalamt beabsichtigt, zukünftig die Betroffenen um Einwilligung zur Übermittlung der Diagnosedaten zu bitten. Eine entsprechende Einwilligungserklärung soll mit mir abgestimmt werden.

16.3 Speicherung falscher Daten zur Staatsangehörigkeit im Melderegister

Eine 18-jährige Bürgerin hat sich bei mir im Berichtsjahr über die unrichtige Speicherung ihrer Daten im Einwohnermelderegister der Stadt Bremerhaven beklagt. Im Zusammenhang mit der Ausstellung eines von ihr für eine Anstellung benötigten Führungszeugnisses war der Bürgerin aufgefallen, dass für sie seit ihrer Geburt neben der deutschen auch eine US-amerikanische Staatsangehörigkeit im Melderegister gespeichert wird. Wie sie mir zu dieser Eintragung erläuternd weiter mitgeteilt hat, sei ihr Vater zwar US-Amerikaner, doch sei eine dementsprechende Staatsangehörigkeit für sie nie beantragt worden. Der Antrag wäre die Voraussetzung für die Erteilung der amerikanischen Staatsangehörigkeit gewesen. Auf ihren mehrfach gegenüber der Meldebehörde geäußerten Einwand, die Speicherung der amerikanischen Staatsangehörigkeit sei unrichtig, habe diese ihr mitgeteilt, die Eintragung sei seinerzeit erfolgt, weil davon auszugehen gewesen war, dass die doppelte Staatsangehörigkeit beantragt wird. Trotz ihres Hinweises, die amerikanische Staatsangehörigkeit sei nie beantragt worden, was die Bürgerin mit einem Schreiben der US-Botschaft in Deutschland auch belegte, war die Meldebehörde zunächst nicht bereit gewesen, die unrichtige Eintragung im Melderegister zu löschen.

Den Meldebehörden kommen in der Verwaltung zentrale Aufgaben von besonderer Bedeutung zu. Es ist für die Einwohnerinnen und Einwohner von hoher Bedeutung, dass die dort verarbeiteten Daten auch richtig sind, man denke nur einmal an Merkmale wie „verheiratet“, „gestorben“ oder „Steuerklasse“. Die Ämter sind verpflichtet, nur richtige Daten über Betroffene zu speichern. Sind gespeicherte Daten unrichtig, haben die Meldebehörden diese Daten bereits von Amts wegen zu berichtigen.

Erst nachdem ich mich mit der Meldebehörde in Verbindung gesetzt habe, hat diese eingeräumt, dass die Eintragung der amerikanischen Staatsangehörigkeit im Melderegister irrtümlich erfolgt sei. Sie hat die Eintragung deshalb gelöscht. Die betroffene Bürgerin hat ein berichtigtes Führungszeugnis erhalten.

17. Datenschutz auf internationaler Ebene

17.1 Internationale Konferenz der Beauftragten für den Datenschutz

Die 30. Internationale Konferenz der Beauftragten für den Datenschutz und die Privatsphäre tagte 2008 vom 15. bis 17. Oktober in Straßburg. Auch hier standen die datenschutzrechtlich aktuellen Themen „Soziale Netzwerke“ und „Schutz der Pri-

vatsphäre von Kindern“ im Mittelpunkt. Der Tenor des schon im Düsseldorfer Kreis gefassten Beschlusses zur datenschutzkonformen Ausgestaltung von sozialen Netzwerken (vgl. Ziff. 21.2) wurde im Wesentlichen von der Internationalen Konferenz übernommen, es wurde eine eigene Entschließung gefasst. Außerdem sprach sich die Internationale Konferenz für die Erstellung internationaler Normen zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten aus.

17.2 Pläne einer Vorratsspeicherung von Flugpassagierdaten

Auf europäischer Ebene wird die Speicherung von Flugpassagierdaten und deren Weitergabe an Drittstaaten kontrovers diskutiert. Die EU-Kommission hat einen Rahmenbeschluss des Europarates vorgelegt, welcher eine solche Vorratsdatenspeicherung vorsieht. Hiernach sollen künftig die Fluggesellschaften bei Flügen aus der EU und in die EU zu jedem Fluggast mindestens 19 Datenelemente an eine von dem jeweiligen Mitgliedstaat bestimmte Zentralstelle übermitteln. Dort sollen die Daten insgesamt 13 Jahre gespeichert werden. Seitens der Bundesregierung werden die EU-Pläne derzeit abgelehnt. Die Justizministerin kündigte an, die Bundesregierung werde das Vorhaben auf europäischer Ebene in der laufenden Legislaturperiode (sprich: bis zur Bundestagswahl im September 2009) verhindern. In so manchem Detail sei keine Relevanz für die Terroristenfahndung zu erkennen.

Diese geplante Vorratsdatenspeicherung verstößt nicht nur gegen Art. 8 der Europäischen Menschenrechtskonvention und gegen die Europaratskonvention 108, sondern ist auch mit dem im Grundgesetz verankerten Recht auf informationelle Selbstbestimmung nicht vereinbar. Aus diesem Grund forderte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung die Bundesregierung auf, den Entwurf abzulehnen (vgl. Ziff. 20.6).

17.3 2. Europäischer Datenschutztag am 28. Januar 2008

Die Europäische Union hat den 28. Januar zum Europäischen Datenschutztag erklärt. Erstmals wurde dieser Tag im Jahr 2007 gefeiert. Für den 2. Europäischen Datenschutztag haben sich die Datenschutzbeauftragten des Bundes und der Länder auf das Schwerpunktthema „Datenschutz aus der Sicht von Schülerinnen und Schülern“ geeinigt. Es wurden eine zentrale Veranstaltung in Berlin und dezentrale Veranstaltungen in den Ländern durchgeführt. So haben Mitarbeiter meiner Dienststelle eine Unterrichtseinheit in einer gymnasialen Oberstufe in Bremerhaven abgehalten und dabei Fragen des Datenschutzes im Bewerbungsverfahren in den Vordergrund gerückt. Auch Datenschutzfragen bei der Internetnutzung, insbesondere der Plattform „schülerVZ“, wurden behandelt.

Das Interesse der Schülerinnen und Schüler war so überraschend positiv, dass ich erwäge, im Rahmen der personellen Möglichkeiten meiner Dienststelle derartige Veranstaltungen zu wiederholen.

18. Datenschutz in der Privatwirtschaft

18.1 Themen der obersten Datenschutzaufsichtsbehörden

Um in allen Bundesländern, aber auch EU-weit, einen einheitlichen Datenschutzstandard zu gewährleisten, ist ein regelmäßiger Informationsaustausch wie auch eine Abstimmung der Praxis unter den Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich erforderlich. Hieran beteilige ich mich regelmäßig. Nachfolgende Themen standen bei den Beratungen in 2008 im Vordergrund, einige davon werden in separaten Punkten dieses Berichts näher ausgeführt. Einen wesentlichen Punkt der Beratungen stellten die verschiedenen Datenskandale dar, beginnend mit der heimlichen Videoüberwachung von Beschäftigten in Discounterketten über verschiedene Internetangebote zum Verkauf von Millionen von Personen- und Adressdaten mit zugehöriger Kontoverbindung, verbunden mit weitreichendem Missbrauch dieser Daten durch Abbuchungen von den Konten im Lastschriftverfahren. Im Zusammenhang mit diesen Datenskandalen standen dann der sog. Datenschutzgipfel und die von den Datenschutzaufsichtsbehörden erarbeiteten Vorschläge zur Verbesserung des Datenschutzes bis hin zur Beratung der Gesetzesvorschläge zur Änderung des Bundesdatenschutzgesetzes (BDSG).

Aber auch mit den Auskunfteien wurden die Gespräche über eine Vielzahl neuer Verfahren, Anschlusspartner und Produkte weitergeführt, so die Auskünfte an Vermieter und die Wohnungswirtschaft, an den Versandhandel oder an Handwerksunternehmen und deren Organisationen.

Auch die Versicherungswirtschaft nahm wieder viel Raum ein mit Fragen um den Einsatz von Scoringverfahren und Bonitätsprüfungen, Fragen der Funktionsausgliederung der Datenverarbeitung auf andere Unternehmen, die Beratung der Entwürfe zu Verhaltensregeln für die Versicherungsunternehmen und nicht zuletzt die Konzeption, der Aufbau und die Integration von Altdaten in das für die gesamte Versicherungswirtschaft neu aufzubauende Hinweis- und Informationssystem (HIS).

Es wurde, anknüpfend an die Gespräche mit der Autoindustrie, die datenschutzrechtliche Beurteilung von elektronischen Informationssystemen in Kraftfahrzeugen weiterentwickelt. Auch verschiedene Anwendungen der Videoüberwachungstechnik, wie beim Einsatz in der Gastronomie, in Einkaufszentren (sog. Shopping-Malls) und in Vernehmungsräumen von Privatdetektiven, waren Gegenstand der Beratung. Die datenschutzrechtliche Einordnung von Geodaten, Gebäudebilddatendanken und im Internet veröffentliche Straßenansichten sowie der Beschluss dazu (vgl. Ziff. 21.4 dieses Berichts) waren ebenso Gegenstand der Beratungen wie Fragen des Datenschutzes bei sozialen Netzen (sog. Online-Communities). Ein Beschluss zur datenschutzkonformen Gestaltung sozialer Netzwerke befindet sich unter Ziff. 21.2 dieses Berichts. Auch zur rechtlichen Einordnung von Internetplattformen mit Beurteilungen einzelner Personen und ihrer beruflichen Leistungen, wie „meinprof.de“ (Beschluss dazu vgl. Ziff. 21.1 dieses Berichts), wurde diskutiert. Schließlich waren verschiedene Fragen des Arbeitnehmerdatenschutzes Gegenstand der Erörterungen, hier speziell auch der Einsatz biometrischer Verfahren, wie Gesichtserkennung und Fingerabdruckscan.

18.2 Digitale Straßenansichten

Als die Fahrzeuge von Google im August 2008 durch die Straßen Bremens fuhren, wurde ich hiervon durch erschrockene Bürgerinnen und Bürger informiert. Ich habe daraufhin eine Pressemitteilung herausgegeben, in der ich die Bremerinnen und Bremern aufklärte und ihnen anbot, sie bei der Verfolgung ihrer Rechte im Falle der Veröffentlichung personenbezogener Daten durch Google zu unterstützen. Mit der Pressemitteilung habe ich aber auch klargemacht, dass ich keine Möglichkeit sehe, zu unterbinden, dass Aufnahmen von Häusern und Straßenansichten gefertigt werden. An dieser Rechtsauffassung hat sich auch nach den Ereignissen in Schleswig-Holstein in der Gemeinde Molfsee nichts geändert. Die dort angestellten verkehrsrechtlichen Überlegungen beinhalten jedenfalls keine Datenschutzfragen.

Zwischenzeitlich haben sich auch die obersten Datenschutzaufsichtsbehörden des Bundes und der Länder mit dem Thema der „Digitalen Straßenansichten“ befasst und haben dazu einen Beschluss gefasst (vgl. 21.4 dieses Berichts). Meine mit o. a. Pressemitteilung getätigten Äußerungen werden darin in vollem Umfang unterstützt. Die Bremer Bürgerinnen und Bürger haben Anspruch darauf, nicht mit Gesicht oder sonst erkennbar online gestellt zu werden, gleiches gilt für Kfz-Kennzeichen. Die Firma Google hat z. B insoweit zugesichert, mit einem Programm die Gesichter von Personen und die Autokennzeichen zu verpixeln. Nach dem Beschluss durch die Aufsichtsbehörden müssen auch die Hausnummern verpixelt werden. Darüber hinaus dürfen gegen den Willen der Betroffenen auch Fassaden nicht im Internet abgebildet werden, eine Silhouette oder ein Negativabzug des Hauses darf aber erhalten bleiben. Der Beschluss sieht dabei vor, dass z. B. Hausbesitzer nicht erst warten müssen, bis die Bilder veröffentlicht werden, sondern sie können sich auch schon im Vorwege gegenüber solchen Firmen erklären. Der Beschluss ist allgemein gefasst und gilt für alle Anbieter solcher Straßenansichten. Der Beschluss wurde aber auch Google zugesandt. Eine Antwort ist von Google bisher nicht eingegangen. Zuständige Aufsichtsbehörde gegenüber Google ist der Hamburgische Datenschutzbeauftragte.

Um die brennenden Fragen der Bremer und Bremerhavener Bevölkerung zu klären, habe ich mich im Oktober 2008 erneut an Google gewandt und um Mitteilung gebeten, ob und ggf. wann in Bremerhaven mit einer Bildaufzeichnung durch die Google-Fahrzeuge und wann mit einer Onlinestellung der Bildsequenzen zu rechnen sei. Google hat mir gegenüber erklärt, noch seien dazu keine Entscheidungen getroffen. Der genaue Termin für die Veröffentlichung der Aufnahmen aus Bremen stehe noch nicht fest. Das Projekt „Straßenansicht“ sei logistisch sehr aufwändig und zudem von der Wetterlage abhängig. Daher könne der Termin zur Veröffentlichung erst kurzfristig festgelegt werden. Aus diesem Grund stehe auch ein genauer Termin für ein etwaiges Befahren von Bremerhaven derzeit noch nicht fest. In die-

sem Jahr würde Bremerhaven jedoch definitiv nicht befahren werden. Google wird bemüht sein, mich im Vorfeld über die geplanten Termine zu informieren.

Ich denke, dies stellt einen ausreichenden Kompromiss dar, gibt er mir doch die Möglichkeit, die Bevölkerung im Land Bremen rechtzeitig über eine bevorstehende Freischaltung im Internet zu informieren. So können diese frühzeitig prüfen, ob die Verpixelungssoftware auch in ihrem Fall ausreichend funktioniert hat. Mir ist klar, dass damit nicht alle Fälle zufriedenstellend abgedeckt werden können, ein Bremer Bürger kann auch in einer anderen Stadt aufgezeichnet worden sein; Bürger anderer Bundesländer können sich während der Bildaufzeichnung gerade in Bremen oder Bremerhaven aufgehalten haben. Aber mehr als das, was in dem Beschluss der obersten Datenschutzaufsichtsbehörden enthalten ist, lässt sich aufgrund der geltenden Rechtslage nach ganz überwiegender Meinung zurzeit nicht erreichen.

Ich habe mich allerdings Google gegenüber dafür eingesetzt, dass das Unternehmen auf einer Internetseite den Aufnahmezeitraum und seine Freischaltungsplanung für die Städte in Deutschland bekannt gibt. Dies würde mehr Transparenz schaffen und würde es auch dem Reisenden ermöglichen, die Bilder anderer Städte vorzeitig zu kontrollieren.

18.3 Bericht aus der Arbeitsgruppe Telekommunikation, Tele- und Mediendienste

Die Datenschutzaufsichtsbehörden müssen sich ständig mit den vielen technischen Entwicklungen auseinandersetzen und tauschen ihre Einschätzungen und Erfahrungen vor allem im Arbeitskreis Medien aus, der in der Regel zweimal im Jahr tagt. Themen im letzten Jahr waren u. a.

— Veröffentlichung von Bewertungen von Lehrern, von Hochschul-Lehrveranstaltungen einzelner Dozenten sowie von Dienstleistungen im Gesundheitsbereich im Internet,

— Zuständigkeiten in den Bundesländern für die Kontrolle der Impressumspflicht und der besonderen Informationspflichten bei kommerzieller Kommunikation,

— Anwendung des TMG und des Staatsvertrages für Rundfunk und Telemedien unter besonderer Berücksichtigung der geänderten Rechtslage,

— Verordnungen zum Telekommunikationsgesetz,

— Änderung der Richtlinie 2002/58/EG,

— Ortung von Mobilfunkteilnehmern in verschiedenen Anwendungen,

— Einhaltung von Datenschutzbestimmungen durch Anbieter von Suchmaschinen,

— Datenschutz in sozialen Netzwerken (studiVZ, schülerVZ, xing, etc.),

— Reputationsdienste im Internet,

— Unfalldatenspeicher im Kfz,

— Arbeit der Internet Task Force der Art.-29-Gruppe,

— Reformentwurf zur E-Privacy-Richtlinie,

— datenschutzrechtliche Bewertung von Google Analytics,

— Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet,

— Anonymisierungsdienste und Vorratsdatenspeicherung,

— datenschutzrechtliche Aspekte des Urheberrechts bei der Nutzung des Internets.

18.4 Gesetzentwürfe der Bundesregierung zur Novellierung des BDSG

18.4.1 Novellierung der Regelungen zum Adresshandel

Am 10. Dezember 2008 hat die Bundesregierung den längst überfälligen Entwurf eines Gesetzes (BR-Drs. 4/09) vorgelegt, mit dem Konsequenzen aus den jüngst bekannt gewordenen Fällen erheblicher Datenschutzverstöße insbesondere im Bereich der Werbewirtschaft und des Adresshandels gezogen werden sollen. Neben der Schaffung eines Systems zertifizierter Selbstkontrolle („Datenschutzauditverfahren“), das in einem eigenen Gesetz verankert werden soll, sind insbesondere

Änderungen des Bundesdatenschutzgesetzes (BDSG) vorgesehen. Im Mittelpunkt der Novellierung des BDSG steht die Abschaffung des sog. Listenprivilegs nach § 28 Abs. 3 Ziff. 3 BDSG, das die Übermittlung oder Nutzung listenmäßig zusammengefasster personenbezogener Daten für Zwecke der Werbung oder Markt- und Meinungsforschung in weitem Rahmen ermöglicht. Auch die noch geltende Widerspruchslösung soll gekippt werden. Nach dem vorliegenden Gesetzentwurf sollen künftig Datenverarbeitung bzw. -nutzung in den Bereichen Adresshandel, Werbung sowie Markt- oder Meinungsforschung dem Grundsatz nach von einer ausdrücklichen Einwilligung des Betroffenen abhängig sein (§ 28 Abs. 3 S. 1 BDSG-E). Allerdings wird dieser datenschutzrechtlich dringend gebotene Ansatz durch großzügige Ausnahmeregelungen in den Folgesätzen (§ 28 Abs. 3 S. 2 – 5 BDSG-E), die zudem aufgrund ihrer unklaren Formulierung erhebliche Auslegungsschwierigkeiten mit sich bringen dürften, deutlich eingeschränkt. Auch die bisher von der Wirtschaft vielfach geübte Praxis einer Koppelung von Vertragsabschluss und Einwilligung in die Datenverwendung bzw. -nutzung soll beschränkt werden (§ 28 Abs. 3 b BDSG-E), wobei auch hier aufgrund der Fassung der Vorschrift die Zielerreichung fraglich bleibt. Vorgesehen ist weiterhin eine Stärkung des bisherigen Werbewiderspruchsrechts nach § 28 Abs. 4 BDSG. Hinzukommen soll ferner eine Informationspflicht nicht öffentlicher Stellen und gleichgestellter öffentlicher Wettbewerbsunternehmen – nicht aber sonstiger öffentlicher Stellen – bei Datenschutzpannen gegenüber den Betroffenen. Diese dem Ansatz nach begrüßenswerte Verpflichtung droht jedoch ins Leere zu laufen, da sie nur für einige bestimmte Datenarten gilt, vor allem aber lediglich im Falle „schwerwiegender" Beeinträchtigungen eingreift – eine dehnbare, erheblichen Auslegungsspielraum schaffende Formulierung. Änderungen sind daneben noch im Bereich der Bußgeldvorschrift (§ 43 BDSG) durch Erweiterung der Bußgeldtatbestände und Erhöhung des Bußgeldrahmens sowie der Möglichkeit einer Gewinnabschöpfung beabsichtigt. Der Entwurf sieht schließlich eine angesichts der aktuellen, dringenden Handlungsbedarf anzeigenden Datenskandale nicht nachzuvollziehende Übergangsfrist von drei Jahren vor. Es spricht also vieles dafür, dass mit der geplanten Neuregelung in der jetzigen Form das Ziel eines wirksamen Schutzes des informationellen Selbstbestimmungsrechts im Bereich des Adresshandels und der Werbewirtschaft nur bedingt erreicht werden kann.

Weitere Vorschläge, um einen effektiven Datenschutz sicherzustellen, wie etwa eine drastische Zurückführung des weiten Ausnahmekatalogs bei der Benachrichtigungspflicht nach § 33 BDSG, eine generelle Kennzeichnungspflicht der Daten zur Offenlegung der Datenflüsse, eine Verbesserung der Kontroll- und Sanktionsbefugnisse der Aufsichtsbehörde, wie sie insbesondere die obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich (Düsseldorfer Kreis) in einem Beschluss gefordert hatten (vgl. Ziff. 21.5), berücksichtigt der Entwurf nicht. Es bleibt zu hoffen, dass die notwendigen Verbesserungen noch im parlamentarischen Gesetzgebungsverfahren erreicht werden können.

18.4.2 Novellierung der Regelungen zu Auskunfteien und Scoring

In der parlamentarischen Warteschleife befindet sich – angesichts des dringenden Handlungsbedarfs wenig verständlich – nach wie vor ein zweiter Gesetzentwurf der Bundesregierung (BT-Drs. 16/10529), mit dem die Regelungen des BDSG der gestiegene Bedeutung der Auskunfteientätigkeit und dem weit verbreiteten Einsatz von Scoringverfahren angepasst, insbesondere die Betroffenenrechte durch mehr Transparenz gestärkt werden sollen (vgl. Ziff. 1.6 dieses Berichts).

18.4.3 Anpassung des Sanktionsrahmens bei Ordnungswidrigkeitsverfahren

Die im Berichtsjahr bekannt gewordenen Datenschutzskandale haben die für den Datenschutz im nicht öffentlichen Bereich zuständigen obersten Aufsichtsbehörden und auch das Bundesministerium des Innern veranlasst, verstärkt eine Ausweitung der Bußgeldtatbestände im Bundesdatenschutzgesetz (BDSG) und eine Erhöhung der nach dem Gesetz möglichen Bußgelder anzustreben. Wie sich herausgestellt hat, reichen die bisherigen Sanktionsmöglichkeiten nicht aus, um die Bürgerinnen und Bürger vor dem Missbrauch ihrer Daten zu schützen. Insbesondere fehlen Bußgeldtatbestände zur Sanktionierung folgender Tatbestände: mangelnde Gewährleistung technischer und organisatorischer Sicherungsmaßnahmen, Nichterstellung eines Verfahrensverzeichnisses, Nichtkenntlichmachung von Videoüberwachung, unbefugte Nutzung personenbezogener Daten, mangelnde Beachtung von Betroffenenrechten, wie z. B. Auskunftsrechte und Benachrichtigungspflichten, Unterlassung

einer Sperrung und Verletzung der Bestimmungen über die Erteilung von Datenverarbeitungsaufträgen. Die Höhe der möglichen Bußgelder, die angemessen zu verhängen sind, hat sich insbesondere bei zu ahnenden schweren Verstößen durch große Unternehmen als zu gering herausgestellt. Wenn ein Bußgeld im Verhältnis zu den mit rechtswidriger Verarbeitung personenbezogener Daten erzielten Gewinnen nur noch als gering („peanuts“) empfunden wird, ist diese gesetzliche Nachregelung dringend erforderlich.

Der jetzt vorgelegte Gesetzentwurf der Bundesregierung sieht zusätzlich zu den bisherigen Tatbeständen u. a. vor, dass ordnungswidrig handelt, wer entgegen § 11 Abs. 2 Satz 2 BDSG einen Auftrag nicht, nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt, als Empfänger ihm übermittelter personenbezogener Daten diese für andere Zwecke nutzt, auch ohne sie wie nach den bislang geltenden Gesetzesbestimmungen an Dritte weiterzugeben, oder entgegen des Widerspruchs des Betroffenen personenbezogene Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung verarbeitet oder nutzt. Für Ordnungswidrigkeiten nach § 43 Abs. 1 BDSG, die bislang mit einer Geldbuße bis zu fünfundzwanzigtausend Euro geahndet werden konnten, soll künftig ein Bußgeld von bis zu fünfzigtausend Euro verhängt werden können; für Ordnungswidrigkeiten nach § 43 Abs. 2 BDSG, die bisher mit einer Geldbuße bis zu zweihunderfünfzigtausend Euro belegt waren, ein Bußgeld von bis zu dreihunderttausend Euro. Außerdem soll die Geldbuße nach dem Gesetzentwurf so festgesetzt werden, dass sie den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigt. Reichen die genannten Beträge hierfür nicht aus, so können sie überschritten werden.

18.4.4 Datenschutzauditgesetz

Der Gesetzentwurf der Bundesregierung wird in diesem Bericht unter Ziff. 3 abgehandelt.

18.5 Landesdatenschutzbeauftragte übernehmen Datenschutzaufsichtsbehörden

Der Landesbeauftragte für Datenschutz des Landes Bremen ist seit Anbeginn gleichzeitig auch Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich. Die Nutzung der damit verbundenen Synergieeffekte trägt wesentlich dazu bei, einen effektiven und gleichmäßigen Schutz der persönlichen Daten der Bürgerinnen und Bürger bei deren Verarbeitung sowohl durch öffentliche Stellen als auch private Stellen zu gewährleisten. Der zunehmende elektronische Datenaustausch zwischen öffentlichen und nicht öffentlichen Stellen, z. B. zwischen Sozialbehörden und privaten Maßnahmeträgern, zwischen Kreditinstituten und Finanzämtern oder Sicherheitsbehörden, sowie die ansteigende Verwendung gleicher technischer Systeme erfordern immer stärker eine einheitliche datenschutzrechtliche Beratung und Kontrolle. Diese Überlegungen machen sich zunehmend auch andere Länder zu eigen. Nachdem bereits im Jahr 2007 dem niedersächsischen und dem sächsischen Datenschutzbeauftragten die Aufgaben der Aufsichtsbehörde übertragen worden sind, ist seit dem 1. Oktober 2008 auch der Landesbeauftragte für Datenschutz Rheinland-Pfalz hiermit betraut worden.

18.6 Datenschutzskandal bei einem Callcenter der Telekom

In der ARD-Sendung „Kriminalreport“ wurde berichtet, dass ein Bremerhavener Callcenter Kundendaten der Telekom unrechtmäßig genutzt haben soll. Nach meinem Kenntnisstand soll ein ehemaliger Mitarbeiter Daten von dem Callcenter entwendet und sie missbräuchlich genutzt haben. Sein Büro befand sich in einer Bremerhavener Wohnung. Zum Zeitpunkt des Bekanntwerdens des Missbrauchs wohnte der Verdächtige allerdings schon nicht mehr in der Wohnung. Er soll sich ins Ausland abgesetzt haben. Insoweit waren mir die Hände für ein weiteres Einschreiten gebunden.

Die Telekom ist als Auftraggeberin der Datenverarbeitung verpflichtet, die Einhaltung datenschutzrechtlicher Anforderungen durch Vereinbarungen und Nachprüfungen bei dem Callcenter sicherzustellen und kann sich nicht durch Auslagerung der Datenverarbeitung ihrer Verantwortung für die Kundendatensätze entziehen. Ich habe mich daher an den Konzernbeauftragten der Telekom sowie den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), welcher für Telekommunikationsunternehmen zuständig ist, gewandt und um Aufklärung gebeten. Der Konzernbeauftragte teilte mir mit, dass die Telekom Strafan-

zeige gestellt habe. Damit obliegt es in erster Linie der Staatsanwaltschaft, den Vorfall aufzuklären und zu ahnden. Der BfDI ist ebenfalls mit der Telekom im Gespräch und versucht, die Ursachen für die diversen Datenschutzprobleme in der letzten Zeit zu ergründen und abzustellen.

18.7 Videoüberwachung

Auch in diesem Berichtszeitraum bin ich wieder auf eine Vielzahl von Videoüberwachungen hingewiesen worden, von denen ich nur drei Fälle wie folgt herausgreife:

18.7.1 Videoüberwachung in einem Erotikkino

Die Polizei Bremen hat erklärt, im Rahmen ihrer Streifentätigkeit sei sie von einem auswärtigen Bürger auf eine Videokamera links oben in der Einzelkabine eines Erotikkinos hingewiesen worden. Daraufhin habe die Polizei festgestellt, dass eine derartige Videokamera dort tatsächlich vorhanden sei, jedoch kein Hinweis darauf. Der Geschäftsführer habe erklärt, Aufnahmen durch die Kamera würden nur dann ausgelöst, wenn am Geldausgabeschlitz in der Kabine manipuliert werde. Nachdem die Polizei mir den Fall zuständigkeitshalber übergab, hat der Geschäftsführer mir auf Anfrage erklärt, er habe die Kamera sofort entfernt. Sollte aber wegen der Aufbrüche noch einmal eine Kamera installiert werden, so werde auf diese für jeden sichtbar hingewiesen.

18.7.2 Videoüberwachung eines Whirlpools

In einer Saunalandschaft in Bremen wurden die Whirlpools im Innen- und im Außenbereich videoüberwacht. Da sich Gäste regelmäßig nackt in Whirlpools begeben, wandte sich ein Beschwerdeführer gegen die Verletzung seiner Intimsphäre. Der Betreiber hat auf meine Anfrage erklärt, die Videoüberwachung erfolge zur Sicherheit der Gäste. Die Videokamera im Innenbereich hat er dann entfernt. Zum Außenbereich hat der Betreiber erklärt, die Videoüberwachung werde zur Abwehr von Einbrüchen etc. nur noch außerhalb der Öffnungszeiten aktiviert; entsprechende Hinweise würden dort angebracht.

18.7.3 Videoüberwachung in einem Einkaufszentrum

Aufgrund eines Hinweises, das Einkaufszentrum Columbus Center in Bremerhaven würde videoüberwacht, ohne dass eine entsprechende Kenntlichmachung erfolgt sei, hat die Betreiberin auf meine Frage nach dem Zweck der Videoüberwachung und die Einhaltung der Vorgaben des § 6 b Bundesdatenschutzgesetz (BDSG) erklärt, die Videoüberwachung erfasse die Drehtüranlagen und Rolltreppen und erfolge überwiegend in der verschlossenen Zeit; inzwischen seien geeignete Hinweise angebracht worden.

18.8 Auskunfteien

18.8.1 Änderung des Bundesdatenschutzgesetzes im Auskunfteienrecht und zu Scoring

In meinem letzten Jahresbericht (vgl. 30. JB, Ziff. 19.3.4) habe ich dargelegt, dass der von der Bundesregierung vorgelegte Änderungsentwurf des Bundesdatenschutzgesetzes (BDSG) zum Auskunfteienrecht zwar einige präzise Regelungen beim Einsatz von Scoringverfahren enthält. Gleichwohl reichen diese Regelungen nicht aus, um die Rechte der Betroffenen hinreichend zu verbessern. Es muss insbesondere gewährleistet werden, dass die bei Auskunfteien gespeicherten Daten nicht zur Erstellung von Persönlichkeitsprofilen Betroffener genutzt werden dürfen. Dies wäre z. B. der Fall, wenn alle Einkommens- und Vermögensverhältnisse sowie die persönlichen Lebensumstände eines Betroffenen gespeichert würden. Außerdem muss präzise geregelt werden, dass die Einholung einer Bonitätsauskunft auch zukünftig an das Vorliegen eines finanziellen Ausfallrisikos geknüpft bleibt. Die als eindeutigen Datenschutzrückschritt zu bewertende im Entwurf vorgesehene Regelung, wonach jedes rechtliche oder wirtschaftliche Interesse, einschließlich der Vermeidung allgemeiner Vertragsrisiken, ein berechtigtes Interesse darstellen kann, würde die Rechte der Betroffenen erheblich und unverhältnismäßig beeinträchtigen. Der Gesetzentwurf schließt nämlich nicht eindeutig genug aus, dass nur solche Unternehmen diese Informationen erhalten dürfen, die Kreditrisiken eingehen, sodass nicht auszuschließen ist, dass sich z. B. sogar Arbeitgeber über die finanziellen Verhältnisse ihrer Beschäftigten informieren. Des Weiteren fehlen

im Entwurf klare Festlegungen, dass nur vertragsrelevante Daten in die Berechung des Scorewerts einbezogen werden dürfen, was die Einbeziehung von z. B. Angaben über das Wohnumfeld des Betroffenen, seines Migrationshintergrundes, Alters oder Geschlechts nicht zulässt. Auch dürfen die Auskunftsrechte der Betroffenen nicht durch die pauschale Berufung auf ein Geschäftsgeheimnis seitens der Auskunftei vereitelt werden.

Der nunmehr an den Bundsrat weitergeleitete Gesetzentwurf der Bundesregierung (BR-Drs. 548/08) vom 8. August 2008 verbessert zwar die Rechte der Betroffenen partiell, leider regelt der Gesetzentwurf nicht präzise genug, dass dem Betroffenen die zur Berechnung seines Scorewerts maßgeblichen Merkmale und ihre Gewichtung mitgeteilt werden. Auch bezieht die in § 28 b BDSG vorgesehene Regelung zu Scoring die Nutzung von Anschriftendaten zur Berechnung des Wahrscheinlichkeitswerts sogar ausdrücklich ein. Durch die Einbeziehung dieser und anderer soziodemografischer Angaben würde die Bonität des Betroffenen auch ohne vertragsrelevante Informationen (z. B. Einkommens- und Vermögensverhältnisse und Zahlungsverhalten) bewertet, wodurch er nicht mehr in der Lage wäre, durch eigenes rechtstreues Verhalten sein Erscheinungsbild zu beeinflussen. Erfreulicherweise hat der Bundesrat hierzu in seiner Stellungnahme eine Änderung beschlossen, wonach besondere Arten von Daten, die an die Anschrift des Betroffenen oder dessen Wohnumfeld anknüpfen sowie Schätzdaten nicht für Berechnung des Wahrscheinlichkeitswerts verwendet werden dürfen (BR-Drs. 548/08 [Beschluss] vom 19. September 2008).

18.8.2 Handels- und Wirtschaftsauskunfteien

Auch im Berichtsjahr erhielt ich wieder mehrere Eingaben, die sich gegen die Datenverarbeitung von Handels- und Wirtschaftsauskunfteien richteten.

Im Wesentlichen kann ich mich dabei auf die Darstellungen in den vergangenen Jahren beziehen, denn die überwiegend gleichen Themen, wie die Richtigkeit der Daten, Umfang der beauskunfteten Daten und Richtigkeit der Bewertung stehen dabei im Vordergrund. Immer wieder beklagten sich Betroffene auch darüber, dass die betreffenden Auskunfteien ihren Auskunftsverlangen nach § 34 Bundesdatenschutzgesetz (BDSG) nicht oder nur teilweise nachkommen oder ihren Ansprüchen auf Berichtigung oder Sperrung der über sie gespeicherten Daten nicht entsprechen. Es gelingt erst oft durch mein Tätigwerden, die Ansprüche der Betroffenen gesetzeskonform durchzusetzen.

Neue Herausforderungen entstehen durch das Wirken von Auskunfteien auf dem Mietermarkt. Erste Beschwerden machen deutlich, dass dadurch benachteiligten Gruppen der Abschluss von Mietverträgen erschwert wird. Ich werde diese Entwicklung beobachten, ggf. ist der Gesetzgeber gefordert, hier klare Grenzen aufzuzeigen. Dabei stelle ich nicht das berechtigte Interesse des Vermieters in Frage, das Mietausfallrisiko zu vermindern. Insoweit ist die Prüfung anzuerkennen, ob der Mietinteressent in der Lage ist, die Miete zu bezahlen. Gleiches gilt dafür, dass der Vermieter sog. schwarze Schafe, wie z. B. Mietnomaden, erkennen möchte.

18.9 Versicherungswirtschaft

18.9.1 Entsorgung von Versicherungsunterlagen im Müllcontainer eines Discounters

Im März des Berichtsjahres meldete sich eine Mitarbeiterin eines Supermarktes in Bremen und teilte mit, dass ein Versicherungsvermittler einer großen Versicherungsgesellschaft Vertragsunterlagen von Kunden in Müllsäcken in den Müllcontainer des Supermarktes verbracht habe. Der Supermarkt hatte den Versicherungsvermittler zur Abholung der Unterlagen aufgefordert und sich mir gegenüber bereit erklärt, die Unterlagen in der Zwischenzeit vor unbefugten Zugriffen zu schützen. Ich rügte den Versicherungsvermittler für sein Vorgehen, welches bei Weitem nicht den Anforderungen an eine datenschutzkonforme Entsorgung von Unterlagen mit teilweise sehr sensiblen personenbezogenen Daten entspricht, forderte ihn mit Nachdruck auf, die Unterlagen beim Supermarkt unverzüglich abzuholen und diese auf datenschutzgerechte Weise zu entsorgen, z. B. zu schreddern. Dies sagte er zu und erklärte, dass die Unterlagen durch ein Missverständnis bei einer großen Aufräumaktion versehentlich mit anderem Müll von seinen Mitarbeitern im Müllcontainer des Supermarktes entsorgt worden seien.

18.9.2 Bericht aus der AG Versicherungswirtschaft

Die Arbeitsgruppe Versicherungswirtschaft tagte im Januar, Februar, Juli und November des Berichtsjahres. Beraten wurden unter anderem die folgenden Themen: Verhaltensrichtlinien der Versicherungswirtschaft, Formulierung von Einwilligungs- und Schweigepflichtentbindungserklärungen, Hinweis- und Informationssystem (HIS) der Versicherungswirtschaft, Versichertenumfrage des PKV, Scoring und Bonitätsabfragen in der Versicherungswirtschaft und Datenweitergabe bei Funktionsübertragung.

18.10 Handel, Handwerk und Dienstleistungen

18.10.1 Erkennen der PINs der EC-Karten über Kassenspiegel in einem Supermarkt

Bemängelt wurde, Kunden in der Warteschleife an der Kasse könnten durch über dem Kassenbereich angebrachte Spiegel die PINs der EC-Karten des Kunden erkennen, der gerade bezahlt. Auf Nachfrage ist mir erklärt worden, die Spiegel erleichterten die Einsichtnahme in den Einkaufswagen durch Kassenmitarbeiter. Ich habe darauf hingewiesen, dass die Eingabe der PIN diskret zu erfolgen hat. Die Spiegel sind daraufhin ersatzlos entfernt worden.

18.10.2 Speicherung der Kreditkartennummer auf der Tankstellenquittung

Immer wieder beschweren sich Bürgerinnen und Bürger darüber, dass auf der Tankstellenquittung die vollständige Scheck- oder Kreditkartennummer sichtbar gespeichert wird. Befürchtet wird, dass diese Nummern durch achtloses Wegwerfen der Quittungen durch Kunden, denen die Kartennummern auf den Quittungen nicht sofort auffallen, unbefugten Personen zugänglich und missbräuchlich verwendet werden könnten.

Auf meine Nachfrage ist mir von dem Unternehmen, das mehrere Tankstellen in Bremen betreibt, erklärt worden, der Kunde erhalte zwei Bons, einen Kassenbon und einen Transaktionsbeleg des Kartenterminals. Ab sofort werde auf der Kreditkartenquittung (Transaktionsbeleg) die Kartennummer durch xxx ersetzt. Die Unkenntlichmachung der Nummer auf dem Kassenbon mache einen kompletten Kartenterminalaustausch notwendig, welcher innerhalb der nächsten drei bis vier Monate durchgeführt werde, sodass das Problem dann behoben sei.

18.10.3 Erhebung der Postleitzahl und Speicherung des Namens des EC-Karteninhabers auf dem Bon

Ein Schuhgeschäft verlangte von Kunden beim Bezahlen der eingekauften Ware die Angabe der jeweiligen Postleitzahl; außerdem wurde auf den Bons der Name des jeweiligen EC-Karteninhabers aufgedruckt.

Auf Anfrage erklärte das Schuhhaus, die Postleitzahl werde nur auf freiwilliger Basis erhoben; der verantwortliche Mitarbeiter habe sich falsch verhalten. Mit Hilfe der Postleitzahl sei es erheblich leichter, bei fehlender Einlösung von Lastschriften die Adresse des betreffenden Kunden zu ermitteln. Das Gleiche gelte für die Speicherung des Namens auf dem Bon. Aufgrund der Eingabe wolle man aber in Zukunft auf die freiwillige Angabe der Postleitzahl und den Namen auf dem Bon verzichten.

18.11 Vereine

Es erreichten mich im Berichtsjahr mehrere Eingaben aus Vereinen. So beschwerte sich zum Beispiel ein Vereinsmitglied über die bevorstehende Datenübermittlung von seinem Verein zu einer Versicherung. Dabei sollten Name und Anschrift an die Versicherung weitergegeben werden, um den Vereinsmitgliedern günstige Konditionen im Rahmen eines Gruppenversicherungsvertrages einzuräumen, den der Verein für seine Mitglieder mit einem Versicherungsunternehmen abgeschlossen hatte. Gemäß § 28 Abs. 3 Nr. 3 Bundesdatenschutzgesetz (BDSG) ist eine Datenübermittlung von Name und Anschrift grundsätzlich für Zwecke der Werbung zulässig. Zur Werbung der schutzwürdigen Interessen der Vereinsmitglieder muss vor einer Datenweitergabe eine Unterrichtung über das Widerspruchsrecht gegenüber den Vereinsmitgliedern erfolgen. Der Verein war sehr kooperativ und wählte den für die Weitergabe der Daten datenschutzfreundlicheren Weg über die Einwilligung. Es bleibt den Vereinsmitgliedern überlassen, in die Datenübermittlung einzuwilligen.

18.12 Gesundheit

18.12.1 Prüfung der Datenverarbeitung in der Physiotherapie

Im Juli des Berichtsjahres überprüfte ich stichprobenartig die Datenverarbeitung durch Physiotherapeuten. Erfreulicherweise begegnete mir von Seiten der überprüften Physiotherapeuten ein angemessenes Datenschutzbewusstsein, sodass ich lediglich auf die Umsetzung einiger weniger Maßnahmen hinwirken musste.

Ich wies darauf hin, dass in den Fällen der Übermittlung von Behandlungsberichten an die verordnenden Ärzte sicherzustellen ist, dass dies in jedem Fall mit Wissen und im Einverständnis der betroffenen Patienten erfolgt.

Das bei einer Praxis eingesetzte Fachverfahren, das die Möglichkeit bietet, differenzierte Zugriffe auf die Daten zu definieren und eine verschlüsselte Speicherung der Daten auf der Festplatte ermöglicht, genügt den datenschutzrechtlichen Anforderungen. Jedoch musste die Fernwartung sowie die Wartung des Praxisnetzes den Anforderungen des § 11 Bundesdatenschutzgesetz (BDSG) entsprechend noch vertraglich geregelt werden. Dazu waren die Sicherheitsmaßnahmen (sichere Authentisierung der Firma, Freischaltung und Kontrollmöglichkeit durch die Praxis etc.) festzulegen und die ausführenden Mitarbeiter der Firma auf das Datengeheimnis gem. § 5 BDSG zu verpflichten für den Fall, dass Patientendaten zur Kenntnis genommen werden. Der Internetanschluss musste noch durch eine Firewall abgesichert werden. Außerdem mussten für im Trainingsbereich elektronisch gespeicherte Patientendaten Löschfristen festgelegt werden.

18.12.2 Datenschutzverletzungen von Ärzten

Dem Datenschutz sollte gerade in Arztpraxen und Krankenhäusern, wo notwendigerweise ständig höchst sensible Gesundheitsdaten verarbeitet werden, ein hoher Stellenwert beigemessen werden. Ein Blick hinter die Kulissen offenbart jedoch gelegentlich, dass Ärzte bei der Organisation der Abläufe in der eigenen Einrichtung weit hinter den in der Öffentlichkeit erhobenen datenschutzrechtlichen Forderungen zurückbleiben.

So wurde ich mit der Frage konfrontiert, ob das Verfahren einer spezialisierten Arztpraxis in Bremen, Behandlungsdaten ohne Vorliegen einer Einwilligungserklärung der Patienten zwischen der Praxis und einer kommunalen Klinik auszutauschen, unbedenklich sei. Die Praxis hatte der Klinik den vollen Zugriff auf den dortigen elektronisch gespeicherten Datenbestand eingerichtet. Ich erklärte, dass es dafür keine Rechtsgrundlage gibt und dies einen Verstoß gegen die ärztliche Schweigepflicht darstellt. Ich klärte darüber auf, dass ein Zugriff der Klinik auf die Behandlungsdaten der Praxis zulässig sei, soweit von den betroffenen Patienten Einwilligungserklärungen eingeholt würden. Die Praxis bestätigte mir kurz darauf, dass die Zugriffsmöglichkeit durch die Klinik aufgehoben worden sei.

Im Juni 2008 wandte sich ein Patient an mich mit dem Hinweis, dass von der Klinik mitgeteilt worden sei, ein Zugriff auf seine Patientendaten in der Arztpraxis sei nicht möglich, weil der Datenschutz dem entgegenstehe. Er bat darum, insoweit über eine Änderung der Datenschutzvorschriften nachzudenken. Ich klärte ihn darüber auf, dass ich seine Arztpraxis schon vor längerer Zeit darüber aufgeklärt hatte, dass entsprechende Zugriffe mit Einwilligung der Patienten zulässig seien. Ich regte an, diese Möglichkeit mit seinem Arzt noch einmal direkt zu besprechen. Hier ist wohl wieder einmal das „Datenschutzargument“ vorgeschoben worden, um einen erhöhten Verwaltungsaufwand abzuwenden.

Im Juli des Berichtsjahres wandte sich eine Patientin einer orthopädischen Praxis an mich und berichtete, dass sie bei einem Besuch in der Arztpraxis im Zusammenhang mit der Verschreibung eines Hilfsmittels vom Arzt ohne nähere Erläuterung an einen Techniker verwiesen worden sei. Dieser Techniker befand sich in einem Raum in der Praxis, sodass die Patientin davon ausgegangen war, dass es sich um einen Mitarbeiter der Praxis handelt. Im Gespräch musste sie dann feststellen, dass es sich um einen Mitarbeiter eines Sanitätshauses handelt, der Zugriff auf ihre Patientendaten hatte, ohne dass sie dafür eine Schweigepflichtentbindungserklärung abgegeben hatte. Auf meine Aufforderung zur Stellungnahme meldete sich der Arzt telefonisch und teilte mit, dass er seit Jahren immer Daten an Apotheken und Sanitätshäuser übermittle, ohne die Einwilligung der betroffenen Patienten einzuholen. Er behauptete, dass eine orthopädische Praxis gar nicht anders zu organisieren sei und dass dies auch im Interesse der Patienten sei. Im Übrigen würden auch alle

anderen Praxen entsprechend verfahren. Ich klärte ihn darüber auf, dass dieses Verhalten einen Verstoß gegen die ärztliche Schweigepflicht darstellt, woraufhin er sich sehr aufregte und zu schimpfen begann. Ich forderte ihn auf, dazu schriftlich Stellung zu nehmen und kündigte an, dass ich als Aufsichtsbehörde die Datenübermittlungen an Dritte ohne Einwilligungserklärung der Betroffenen untersagen würde. Sollten ihm andere Praxen bekannt sein, die entsprechend verfahren, so könne er mir diese nennen, damit ich mich ebenfalls an diese wenden könnte. In seiner schriftlichen Stellungnahme stritt der Arzt dann alles ab und gab an, alle Patienten auf die Tatsache der Zusammenarbeit mit einem Fremdunternehmen und die Freiwilligkeit ihrer Teilnahme hinzuweisen.

18.13 Arbeitnehmerdatenschutz

18.13.1 Schaffung eines Arbeitnehmerdatenschutzgesetzes

Angesichts der verschiedenen Vorfälle von Arbeitnehmerüberwachung (vgl. Ziff. 18.13.4 dieses Berichts) in Unternehmen und der für Arbeitgeber wie Arbeitnehmer unübersichtlichen Gesetzeslage zum Arbeitnehmerdatenschutz, hat der Bundesrat am 7. November 2008 auf Initiative des Landes Rheinland-Pfalz eine Entschließung zur gesetzlichen Ausgestaltung des Arbeitnehmerdatenschutzes gefasst (BR-Drs. 665/08). Erreicht werden soll, dass Arbeitnehmer und Arbeitgeber ihre Rechte und die Grenzen des Umfangs und der Verwendung von Arbeitnehmerdaten kennen. Dieses sei nur mit übersichtlichen gesetzlichen Regelungen zu gewährleisten. Die bestehenden Regeln zum Datenschutz in Arbeitsverhältnissen entsprächen diesen Anforderungen nicht. Erforderlich seien praktikable, verständliche gesetzliche Regelungen, die die Prinzipien der Transparenz, der Erforderlichkeit und Verhältnismäßigkeit, der legitimen Zweckbindung wie auch der Datensparsamkeit und Datensicherheit berücksichtigen. Kernelement eines effektiven Arbeitnehmerdatenschutzes müsse die sachgerechte Begrenzung der Verarbeitung von Arbeitnehmerdaten sein mit strengen Zweckbindungs- und Verwertbarkeitsregelungen. Ebenso grundlegend sei auch die Achtung der grundgesetzlich geschützten Persönlichkeitsrechte (vgl. 30. JB, Ziff. 1.6 und 21.5).

Obwohl im Kern dieser Auftrag an die Bundesregierung seit langem existiert, hat sie anlässlich der Beratungen in der Sitzung des Bundesrats dazu erklärt, angesichts der Komplexität des Vorhabens sei in der laufenden Legislaturperiode des Bundestages die Verabschiedung eines umfassenden und einheitlichen Arbeitnehmerdatenschutzgesetzes nicht mehr zu verwirklichen.

18.13.2 Beratung von Betriebsräten

Im Berichtszeitraum hat sich die Anzahl an Beratungen von Betriebsräten erheblich gesteigert. Dies liegt offensichtlich an dem zunehmenden Informationsfluss im Betrieb und damit einhergehenden Datenschutzproblemen im Zusammenhang mit der Überwachung der Beschäftigten und dem gestiegenen Datenschutzbewusstsein der Betriebsräte. Zu ihren originären Aufgaben nach § 80 Betriebsverfassungsgesetz (BetVG) gehört u. a., die Einhaltung der zugunsten der Beschäftigten bestehenden Rechtsvorschriften zu überwachen, also auch der Datenschutzbestimmungen. Da der Betriebsrat Teil der verantwortlichen Stelle ist, gehört diese Beratung auch zu meinen gesetzlichen Aufgaben nach § 38 Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG), wonach ich die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse zu beraten und zu unterstützen habe.

Insbesondere folgende Themen wurden im Rahmen der einzelnen Beratung von Betriebsräten behandelt:

— Internet und E-Mail und die Kontrollbefugnisse des Arbeitgebers,

— Aufbewahrung und Verwaltung von Beschäftigtendaten,

— Elektronische Schlüssel (Transponder) und deren Datenverarbeitung,

— Arbeitseinsätze und Dienstpläne über den PC per Intranet,

— Aufgaben und Voraussetzung zur Bestellung von Beauftragten für den Datenschutz,

— Information der Beschäftigten über die Personaldatenverarbeitung im Betrieb,

— Zugang zu Daten des Betriebsrats (z. B. E-Mail-Programm) durch den Administrator,

— Aufbewahrung von Betriebsratsprotokollen, Anhörungen etc.,

— Datenschutzerklärungen von Betriebsratsmitgliedern.

18.13.3 Digitale Unterschriften der Beschäftigten

Auf eine Anfrage habe ich mitgeteilt, dass die Verwendung digitaler Unterschriften der Beschäftigten zulässig ist, soweit sie für einen wirtschaftlichen Geschäftsablauf, insbesondere bei Massengeschäften, erforderlich ist und entgegenstehende schützwürdige Interessen nicht überwiegen. Hierzu sollten im Rahmen einer Vorabkontrolle durch den Beauftragten für den Datenschutz des Unternehmens technische und organisatorische Maßnahmen festgelegt werden, die sicherstellen, dass nur der jeweilige Beschäftigte selbst über die Verwendung seiner digitalen Unterschrift entscheidet, wie dies bei der manuellen Unterschrift geschieht. In einer Betriebsvereinbarung oder einer betriebsinternen Regelung sollten der Zweck der digitalen Unterschrift, die alleinige Verfügbarkeit darüber durch den jeweiligen Arbeitnehmer und ggf. Maßnahmen zur Sicherung, dem Ausschluss der missbräuchlichen Verwendung und deren Ahndung festgelegt werden.

18.13.4 Videoüberwachung von Beschäftigten

Im Frühjahr 2008 ist in den Medien ausführlich über die bundesweite Videoüberwachung von Beschäftigten bei Lidl berichtet worden, die im Auftrag des Unternehmens durch Detekteien vorgenommen wurde. Auch in Bremen und Bremerhaven hat es solche heimlichen Videoüberwachungsmaßnahmen gegeben. Die hier ansässigen Filialen gehören einer Lidl-Regionalgesellschaft an, die ihren Sitz bei Schwanewede, also in Niedersachsen, hat, sodass ich nicht zuständig bin. Die Feststellungen der zuständigen Datenschutzaufsichtsbehörde in Niedersachsen haben ergeben, dass die Lidl-Filialen in den Bremer Stadtteilen Gröpelingen und Huchting sowie im Bremerhavener Stadtteil Geestemünde überwacht wurden. Darüber hinaus hat mich die federführende Aufsichtsbehörde des Landes Baden-Württemberg, in dem sich der Hauptsitz von Lidl befindet, um Prüfung bei einer Detektei mit Sitz in Bremen gebeten, weil diese im Auftrag von Regionalgesellschaften mit Sitz in verschiedenen Bundesländern dortige Lidl-Beschäftigte videoüberwachte. Die Prüfung hat ergeben, dass die Detektei von der jeweiligen Regionalgesellschaft kurzfristig darüber unterrichtet wurde, in welcher Filiale und zu welchen Zeiten welche Kassenbereiche zu überwachen sind. Es wurden dann außerhalb der Geschäftszeiten Miniaturkameras an der Decke der Filiale so angebracht, dass sie z. B. die Kassen und damit die Beschäftigten erfassen konnten. Die Videoüberwachung dauerte meistens eine Woche und war teilweise auf bestimmte Beschäftigte konzentriert. Die Bilddaten wurden dann gesichtet und für Berichte an die Regionalgesellschaft verwendet. Das Bildmaterial wurde dem Bericht beigefügt. Unterlagen oder Kopien der Videoaufzeichnungen hatte die Detektei nach ihren Angaben nicht mehr.

Unabhängig davon, dass den Lidl-Regionalgesellschaften insgesamt Bußgelder in Millionenhöhe auferlegt worden sind und bei den Detekteien von derartigen Verfahren Abstand genommen worden ist, unterliegen auch Detekteien den Bestimmungen des Bundesdatenschutzgesetzes (BDSG), wenn sie im Auftrag eines Unternehmens per Videoüberwachung personenbezogene Daten verarbeiten. Die Detektei hat daher auf meine Frage erklärt, sie würde zukünftig die Vorgaben des BDSG einhalten.

Durch die Berichterstattung über die Videoüberwachung bei Lidl haben mich viele Anfragen von Beschäftigten aus Bremen und Bremerhaven erreicht. Einerseits haben sie mit oder ohne Nennung ihres Namens über eine vermutete oder tatsächliche Videoüberwachung in ihren Betrieben berichtet; andererseits haben die meisten – wohl aus Angst vor innerbetrieblichen Repressalien – den Betrieb nicht nennen wollen. In den Fällen, in denen mir die Namen der Unternehmen genannt worden sind, in denen Mitarbeiter videoüberwacht werden, bin ich derzeit dabei, Prüfungen vorzunehmen und zu veranlassen, die unzulässige Videoüberwachung einzustellen bzw. datenschutzkonform umzugestalten, und in eklatanten Fällen Bußgelder zu verhängen.

Hier nur einige Beispiele: In einem Betrieb würden Beschäftigte über Kameras im Treppenhaus, die auch die Toilettentüren erfassen, sowie in der Werkstatt und über das Fenster des Aufenthaltsraums videoüberwacht. Der dortige Geschäftsführer könne per Knopfdruck feststellen, wer sich gerade in welchem Bereich aufhielt. Er habe sogar einen Beschäftigten ermahnt, weil er mit einem Kaffeebecher im Trep-

penhaus gelaufen sei. Außerdem habe dieser Geschäftsführer anderen Beschäftigten gegenüber Anmerkungen zum Arbeitsablauf gemacht, deren Kenntnis nur durch Einsicht in die Videoaufnahmen möglich gewesen sei.

In einer Apotheke wurden die Beschäftigten gezielt im Labor- und Kassenbereich videoüberwacht, ebenso z. B. in einem Restaurant, einem Café oder einem Frisiersalon. Ich bin bemüht, die vielen Beschwerden abzuarbeiten und die Prüfungen zeitnah und effektiv durchzuführen.

18.13.5 Auskunft über einen Erfahrungsbericht durch den Arbeitgeber sowie Recht auf Einsicht in Personalakten

Ein ehemaliger Beschäftigter eines Unternehmens hat moniert, sein damaliger Arbeitgeber sei nicht bereit, ihm eine Kopie des ihn betreffenden Erfahrungsberichts an die Bremer Arbeitsgemeinschaft für Integration und Soziales (BAgIS) zur Verfügung zu stellen; es sei ihm lediglich Einsicht in diesen Bericht gewährt worden. Des Weiteren sei ihm Einsicht in seine Personalakten verwehrt worden.

Auf meine Anfrage hat der Arbeitgeber erklärt, ihm sei klar, dass der Betroffene einen Rechtsanspruch auf beides habe. Da seine hier involvierten Mitarbeiter nicht über die erforderlichen Kenntnisse verfügten und ihn in dieser Angelegenheit nicht zu Rate gezogen hätten, hat er zugesagt, dem Begehren des Petenten nunmehr zu entsprechen.

18.13.6 Führen einer Liste über Rauchpausen

Die Anfrage, ob es zulässig sei, Aufzeichnungen über Rauchpausen betriebsöffentlich in dem Raucherbereich auszulegen, habe ich wie folgt beantwortet:

Arbeitsunterbrechungen – gleich welcher Art – sind Personaldaten, die nur befugten Personen zugänglich sein dürfen, in der Regel dem Beschäftigten, dessen Vorgesetztem bzw. Arbeitgeber und ggf. der Personalabteilung. Die betriebsöffentliche Auslegung einer Liste, in die sich Raucher eintragen sollen, würde bedeuten, dass andere Personen – ob sie dort eine Raucherpause machen oder nicht – Kenntnis über die Rauchpausen erhalten, obwohl dies nicht erforderlich ist. Zudem könnten Raucher dadurch gebrandmarkt werden und der Arbeitgeber erhielte eine Liste über die rauchenden Beschäftigten, ohne dass dazu eine Notwendigkeit bestünde. Insoweit überwiegen schutzwürdige Interessen der Betroffenen gegenüber dieser Datenverarbeitung, unabhängig davon, dass die Liste und deren betriebsöffentliche Auslegung nicht erforderlich ist. Soweit Rauchpausen als Arbeitsunterbrechung gelten, reicht es aus, wenn die Beschäftigten selbst in ihrem Arbeitzeitnachweis Rauchpausen als allgemeine Arbeitsunterbrechung eintragen und Einsicht in die Arbeitszeitnachweise nur befugte Personen erhalten.

18.14 Ordnungswidrigkeitsverfahren in Bremen

Im Berichtszeitraum verhängte ich drei Bußgeldbescheide. In einem der Fälle erließ ich einen Bußgeldbescheid wegen eines Verstoßes gegen die Meldepflicht nach § 4 d BDSG. Mehrfach hatte ich ein Detektei- und Auskunfteiunternehmen zuvor ausgefordert, eine Meldung zu dem von mir nach § 38 Abs. 3 BDSG zu führenden Register abzugeben. Gegen meinen Bußgeldbescheid hat die Detektei und Auskunftei ohne eine Begründung Einspruch eingelegt. Da trotz der fehlenden Begründung der Einspruch nicht zurückgewiesen werden kann, musste der Vorgang zur weiteren Bearbeitung an die Staatsanwaltschaft abgegeben werden. In einem weiteren Fall erging ein Bußgeldbescheid wegen der unbefugten Erhebung von Daten, die nicht allgemein zugänglich sind, durch einen Rechtsanwalt. Dieser hatte bei der Einsichtnahme in eine staatsanwaltschaftliche Ermittlungsakte auch Daten einer unbeteiligten Person erhoben, wozu er nicht berechtigt gewesen war. Die Akteneinsicht war dem Anwalt nur im Rahmen seiner Tätigkeit für einen Mandanten gewährt worden, der unbeteiligte Dritte war von dem Mandat nicht umfasst. Der Bußgeldbescheid ist in diesem Fall rechtskräftig geworden. Der Rechtsanwalt hat das Bußgeld gezahlt. Außerdem erließ ich im Berichtsjahr noch einen Bußgeldbescheid wegen der Nichterteilung mehrmals angemahnter Auskünfte. Ein bundesweit operierendes Unternehmen war in diesem Fall nicht bereit, Auskünfte zur Einholung von Informationen über einen seiner Mitarbeiter bei einer Wirtschaftsauskunftei zu erteilen. Gegen den Bußgeldbescheid wurde Einspruch eingelegt. Der Vorgang wurde daher zur weiteren Bearbeitung an die Staatsanwaltschaft abgegeben. Insgesamt sind von mir Bußgelder in Höhe von zusammen 3600,– Euro verhängt worden.

19. Schlussbemerkungen

19.1 Pflege und Entwicklung der Homepage

Die Seiten meiner Homepage zum Datenschutz sind im Berichtsjahr von 168 000 Usern besucht worden. Um einen genaueren Überblick über die Anzahl der Zugriffe zu erhalten, habe ich im Januar einen Zähler auf meiner Homepage eingefügt, danach teilen sich die Zugriffe wie folgt auf: www.datenschutz.bremen.de mit rund 163 000 und www.datenschutz4school.de mit rund 5000 Usern.

Auf den Seiten www.datenschutz.bremen.de sind u. a. eine Orientierungshilfe für Gerichtsvollzieher sowie verschiedene Beiträge zu aktuellen Themen neu hinzugekommen. So habe ich die Datenschutzskandale und die daraus resultierenden Anfragen der Bürger zum Anlass genommen, unter „Tipps für Bürger“ Ratschläge „Wie kann ich mich vor Datenmissbrauch schützen“ zu veröffentlichen und behandle folgende Fragestellungen:

— Wer sagt mir eigentlich, welche Daten über mich in irgendwelchen Datenbanken liegen?

— Dürfen Firmen oder Behörden einfach meine Daten speichern und weitergeben?

— Woher haben Einrichtungen, die ich manchmal selbst gar nicht kenne, meine Daten?

— Warum können Datenschützer solche Praktiken nicht stoppen?

— Was kann ich denn tun, um meine Daten wenigstens künftig zu schützen?

— Dürfen Verträge oder Geschäfte gekoppelt werden an eine Preisgabe von Daten?

— Kann ich denn meine bereits verfügbaren Daten irgendwie pauschal blockieren?

— Ich erhalte oft Anrufe mit irgendwelchen Werbeangeboten. Muss ich das hinnehmen?

— Wie verhalte ich mich bei solchen unerwünschten Werbeanrufen?

— Ein Werbeanrufer hat mich überrumpelt und mir was aufgeschwatzt? Was nun?

— Oft werden Kontodaten verlangt, gibt es da keinen Schutz?

— Wie verhalte ich mich, wenn unerwünschte Abbuchungen geschehen sind?

— Kann ich eigentlich Datendiebe irgendwie zur Rechenschaft ziehen?

Im November habe ich eine Aufklärungsreihe zum Thema „Profilbildung“ gestartet, die Themenstellung wurde parallel in den Bremer Tageszeitungen aufbereitet. Die Serie beschäftigt sich mit den Daten, die jeder gewollt oder ungewollt von sich preisgibt und die, zu „Profilen“ geformt, sich vermarkten lassen. In der heutigen Zeit, wo jeder Webseiten erstellen und anbieten kann, können Daten über andere Personen mit sehr einfachen technischen Mitteln gesammelt werden. Das geschieht oft, um Informationen abzugreifen, zu verkaufen und damit Geld zu verdienen. Weit über Internet, E-Mail oder Telefon hinaus ist Datenhandel längst zu einem lukrativen und boomenden Wirtschaftszweig geworden. Der Unwissenheit und Leichtgläubigkeit der Betroffenen soll entgegengewirkt werden.

Ob am Computer eine Internetsuchmaschine genutzt oder „online“ eingekauft wird, ob „gebloggt“ wird oder ob man sich an sogenannten sozialen Netzwerken (studiVZ, xing, schülerVZ) beteiligt, ob aus dem Kaufhaus Waren mit aktiven Funkchips nach Hause genommen werden oder Rabattkartensysteme Konsumgewohnheiten protokollieren, ob über DSL-Leitungen Fernsehprogramme empfangen oder Fernsehapparate zum Internet-PC gemacht werden, ob digitale Stempeluhren bedient oder demnächst die Gesundheitskarte benutzt werden, gleichgültig, was getan wird: Jeder produziert Daten und gibt sie preis – Daten, die andere sammeln, auswerten, bündeln, verkaufen oder missbrauchen können. Die Serie soll den Bürgerinnen und Bürgern Hilfe beim Umgang mit den Medien geben und zeigen, wie sie künftig ihre Daten besser schützen.

Die Artikelserie behandelt die folgenden Themen: Google und andere Suchmaschinen, ID-Management, Location Based Services, RFID, Ubiquitäres Computing, Konvergenz von Techniken und Netzen, Soziale Netzwerke – Web 2.0.

19.2 Schriftliche Eingaben und telefonische Anfragen

Im Berichtsjahr stieg die Zahl der schriftlichen Eingaben, die ich per Brief, Telefax oder E-Mail erhielt, sowie der telefonischen Anfragen von Bürgerinnen und Bürgern, die die Datenverarbeitung von Behörden, Unternehmen und anderen Stellen betrafen, in erheblichem Umfang erneut an. Eine eklatante Steigerung, betreffend die Privatwirtschaft, ergab sich in der zweiten Jahreshälfte insbesondere in den Phasen, in denen in den Medien über Datenpannen und Datenklau berichtet wurde. Man kann wohl sagen: tageweise stand das Telefon nicht still. Dabei kann man die Sorgen der Bürgerinnen und Bürger nicht innerhalb weniger Minuten zerstreuen. Insbesondere dann nicht, wenn schnelle Hilfe geboten ist, etwa, weil schon verschiedene Beträge von deren Konten abgebucht wurden.

Bei einem besonders hohen Anteil handelte es sich hier erneut um Fragen, die den Arbeitnehmerdatenschutz zum Gegenstand hatten. Besonders hoch war auch die Zahl der Eingaben und Beschwerden, die Einzelhandels- oder andere Handelsunternehmen betrafen. In diesen wie auch in anderen Bereichen machte sich die rapide Zunahme von Eingaben zur Videoüberwachung besonders bemerkbar. Von zunehmendem Gewicht waren darüber hinaus auch technische Fragestellungen, die die Internetkommunikation betreffen.

Im öffentlichen Bereich betrafen die Eingaben – wie bereits im Vorjahr – insbesondere die Sozialdatenverarbeitung durch die BAgIS, Personaldatenverarbeitung und die Verarbeitung personenbezogener Daten durch die Polizei.

In einer als Anlage beigefügten Tabelle (vgl. Ziff. 23.2 dieses Berichts) habe ich für diesen Bericht wieder eine Auswahl der telefonischen Anfragen, die ich im Berichtsjahr erhielt und die bereits im Telefongespräch mit dem Anrufer beantwortet werden konnten, zusammengestellt.

19.3 Öffentlichkeitsarbeit, Vorträge, Fortbildungsangebote und Kooperationen

In einer globalen und vernetzten Welt ist die Gewährleistung eines effektiven Datenschutzes maßgeblich für die freie und selbstbestimmte Entfaltung des Einzelnen. Nur wenn die Menschen über ihre Rechte umfassend informiert sind, werden sie diese im Hinblick auf die Gestaltung einer demokratischen Informationsgesellschaft auch tatsächlich wahrnehmen können. Zu meinen vordringlichen Anliegen bei der Erfüllung meiner Aufgaben gehört deshalb auch die Information und Beratung der Bürgerinnen und Bürger zu allen Themen des Datenschutzes. Ein immer wichtiger werdendes Instrument ist hierbei das Internet, dessen Nutzerzahl stetig ansteigt. Mein Internetangebot habe ich auch im Berichtsjahr erheblich weiterentwickelt (vgl. Ziff. 11.1 dieses Berichts). Zur Information und Beratung habe ich darüber hinaus im März 2008 eine neue Broschüre zum Datenschutz herausgegeben, in der die Texte des Bremischen Datenschutzgesetzes, der Bremischen Datenschutzauditverordnung und des Bundesdatenschutzgesetzes verbunden mit einer umfangreichen Einführung in die Anwendung der Gesetze veröffentlicht worden sind.

Zur Unterrichtung über datenschutzrechtliche Fragestellungen und Anforderungen haben meine Mitarbeiterinnen und Mitarbeiter des Weiteren auch im Berichtsjahr Fortbildungsmaßnahmen im Aus- und Fortbildungszentrum der bremischen Verwaltung durchgeführt. Die Workshops im Frühjahr und Herbst dieses Jahres haben sich inhaltlich insbesondere mit der Wahrnehmung der Aufgaben der behördlichen Datenschutzbeauftragten und der Organisation und Gestaltung des Datenschutzes in der Behörde befasst. Für den Workshop im Frühjahr des Berichtsjahrs habe ich zwei bereits seit mehreren Jahren im Umland Bremens, der „Region Nordwest“, tätige und sehr engagierte kommunale Datenschutzbeauftragte für Vorträge und Diskussionsrunden gewinnen können (vgl. Ziff. 2.1 dieses Berichts).

Des Weiteren hatte eine Mitarbeiterin meiner Dienststelle an mehreren Diskussionsrunden zum Thema „Kindeswohl und Datenschutz bei Kinderärzten“ teilgenommen.

Die Zusammenarbeit mit den Datenschutzbeauftragten des Bundes und der Länder, mit den obersten Datenschutzaufsichtsbehörden in den unterschiedlichen Gremien, mit Verbänden und anderen Organisationen ist von mir intensiv fortgesetzt worden.

Ein wichtiges Instrument zur Information der Öffentlichkeit, um auf aktuelle Themen zu reagieren, ist die Pressearbeit. In einer Artikelserie in der Bremer Tages-

zeitung im Herbst des Berichtsjahrs habe ich dabei u. a. ausführlich über Risiken und Gefährdungen informiert, die insbesondere mit der Nutzung technischer Neuerungen verbunden sind. Die von mir herausgegebenen Pressemitteilungen sind auf meiner Internetseite veröffentlicht. Einen Auszug über im Berichtsjahr erschienene Zeitungsartikel mit Datenschutzthemen oder mit Datenschutzbezug habe ich wieder im Anhang aufgenommen (vgl. Ziff. 23.2 dieses Berichts). Insbesondere die Datenschutzskandale haben dazu geführt, dass die Zahl der Interviews in der lokalen Presse, in Hörfunk und Fernsehen erheblich angestiegen ist.

19.4 Zur Situation der Dienststelle

Auch im Berichtsjahr mussten in meiner Dienststelle wieder Ausfälle im personellen Bereich überbrückt werden. So musste z. B. die Abordnung eines Referenten zum Datenschutzreferat im Bundesministerium des Innern verkraftet werden. Durch hilfreiche Unterstützung der Senatskommissarin für den Datenschutz konnte der Fehlbedarf noch vor der Sommerpause ausgeglichen werden. Am Ende des Jahres steht meine Dienststelle so gut wie seit Jahren nicht mehr da. Die Referate der Dienststelle sind besetzt und auch für die Informationsfreiheit, die sonst nur zu Lasten des Datenschutzes bedient werden konnte, steht eine halbe Stelle zur Verfügung. Auch die finanzielle Situation hat sich bei knappem Wirtschaften entspannt, sodass ich rechnerisch für 2008 einen ausgeglichenen Haushalt vorweisen kann. Diese seit Jahren erstmals wieder positiv ausfallende Bilanz wurde vor allem durch die Unterstützung aus dem Hause der Senatskommissarin für den Datenschutz möglich.

20. Die Entschließungen desr Datenschutzkonferenzen im Jahr 2008

20.1 Mehr Augenmaß bei der Novellierung des BKA-Gesetzes

(Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3. bis 4. April 2008)

Der vom Bundesministerium des Innern erarbeitete Referentenentwurf eines Gesetzes zur Abwehr des internationalen Terrorismus durch das Bundeskriminalamt hat zum Ziel, das Bundeskriminalamt mit umfassenden polizeilichen Befugnissen zur Verhütung von terroristischen Straftaten und zur Abwehr von Gefahren für die öffentliche Sicherheit in diesem Zusammenhang auszustatten. Insbesondere sind Befugnisse zur Durchsuchung, Rasterfahndung, Wohnraumüberwachung und Telekommunikationsüberwachung vorgesehen. Außerdem will das Bundesinnenministerium eine Befugnis zum heimlichen Zugriff auf informationstechnische Systeme („Onlinedurchsuchung") in das BKA-Gesetz aufnehmen.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dagegen aus, dass dem Bundeskriminalamt nach dem Gesetzentwurf mehr Befugnisse eingeräumt werden sollen, als einzelnen Landespolizeien zur Erfüllung ihrer eigenen Gefahrenabwehraufgaben zustehen. Sie halten es daher für geboten, im weiteren Gesetzgebungsverfahren die Befugnisse des BKA auf die zur Aufgabenerfüllung zwingend notwendigen Kompetenzen zu beschränken.

Die bisherige informationelle Gewaltenteilung zwischen den Polizeien der Länder und dem BKA diente auch dem Datenschutz. Die Konferenz fordert deshalb eine klare, d. h. hinreichend trennscharfe Abgrenzung der spezifischen Befugnisse des Bundeskriminalamts einerseits zu denen der Landespolizeien und Verfassungsschutzbehörden andererseits.

Dem Referentenentwurf zufolge soll die Aufgabenwahrnehmung durch das Bundeskriminalamt die Zuständigkeit der Landespolizeibehörden auf dem Gebiet der Gefahrenabwehr unberührt lassen. Dies führt zu erheblichen datenschutzrechtlichen Problemen, da nach geltendem Recht auch die Länder bei Abwehr einer durch den internationalen Terrorismus begründeten Gefahr parallele Abwehrmaßnahmen ergreifen können. Angesichts der Weite der für das Bundeskriminalamt vorgesehenen und den Landespolizeibehörden bereits eingeräumten Datenerhebungs- und Datenverarbeitungsbefugnisse steht zu befürchten, dass es zu sich überlappenden und in der Summe schwerwiegenderen Eingriffen in das informationelle Selbstbestimmungsrecht Betroffener durch das Bundeskriminalamt und die Landespolizeibehörden kommen wird.

Ebenso stellt sich die grundsätzliche Frage der Abgrenzung von Polizei und Verfassungsschutz. In den vergangenen Jahren sind die Polizeigesetze des Bundes und der Länder zunehmend mit Befugnissen zur verdeckten Datenerhebung (z. B. heimliche Video- und Sprachaufzeichnungen, präventive Telekommunikationsüberwachung) ausgestattet worden. Zudem wurden die Eingriffsbefugnisse immer weiter ins Vorfeld von Straftaten und Gefahren erstreckt. Damit überschneiden sich die polizeilichen Ermittlungsbefugnisse zunehmend mit denen des Verfassungsschutzes.

Das Bundesverfassungsgericht hat in seinem Urteil zur „Onlinedurchsuchung" vom 27. Februar 2008 den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung zu gewährleisten. Diese Vorgabe des Gerichts gilt nicht nur für eine etwaige gesetzliche Regelung zur „Onlinedurchsuchung", sondern für alle Eingriffsmaßnahmen. Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber deshalb auf, im Rahmen der Novellierung des BKA-Gesetzes den Schutz des Kernbereichs privater Lebensgestaltung für alle Eingriffsmaßnahmen zu regeln.

20.2 Unzureichender Datenschutz beim deutsch-amerikanischen Abkommen über die Zusammenarbeit der Sicherheitsbehörden

(Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3. bis 4. April 2008)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beobachtet mit Sorge, dass die Datenschutzrechte der Bürgerinnen und Bürger im Rahmen der internationalen Zusammenarbeit der Sicherheitsbehörden immer häufiger auf der Strecke bleiben. Aktuelles Beispiel ist das am 11.3.2008 parafierte deutsch-amerikanische Regierungsabkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität. Die Konferenz fordert Bundestag und Bundesrat auf, dem Abkommen so lange nicht zuzustimmen, bis ein angemessener Datenschutz gewährleistet ist.

Mit dem Abkommen wurde ein gegenseitiger Onlinezugriff auf Fundstellendatensätze von daktyloskopischen Daten und DNA-Profilen im Hit/no-hit-Verfahren nach dem Muster des Prümer Vertrages vereinbart. Zudem wurden dessen Regelungen über den Austausch personenbezogener Daten zur Verhinderung terroristischer Straftaten weitgehend übernommen. Eine Übertragung des als Bedingung für diese umfangreichen Zugriffs und Übermittlungsbefugnisse im Prümer Vertrag geschaffenen Datenschutzregimes erfolgte jedoch nicht.

Die Voraussetzungen, unter denen ein Datenaustausch erlaubt ist, sind nicht klar definiert. Der Datenaustausch soll allgemein zur Bekämpfung von Terrorismus und schwerer Kriminalität möglich sein. Welche Straftaten darunter konkret zu verstehen sind, wird nicht definiert. Es erfolgt hier lediglich der Verweis auf das jeweilige nationale Recht. Damit trifft nach dem Abkommen die USA einseitig eine Entscheidung über die Relevanz der abgerufenen Daten.

Bevor in so großem Umfang zusätzliche Datenübermittlungen erlaubt werden, muss zunächst geklärt werden, warum die bisherigen Datenübermittlungsbefugnisse für die internationale Polizeizusammenarbeit mit den USA nicht ausreichen.

Für die weitere Verarbeitung aus Deutschland stammender Daten in den USA bestehen für die Betroffenen praktisch keine Datenschutzrechte. Das Abkommen selbst räumt den Betroffenen keine eigenen Rechte ein, sondern verweist auch hierzu auf die Voraussetzungen im Recht der jeweiligen Vertragspartei. In den USA werden aber Datenschutzrechte, wie sie in der Europäischen Union allen Menschen zustehen, ausschließlich Bürgerinnen und Bürgern der Vereinigten Staaten von Amerika und dort wohnenden Ausländerinnen und Ausländern gewährt. Anderen Personen stehen Rechtsansprüche auf Auskunft über die Verarbeitung der eigenen Daten, Löschung unzulässig erhobener oder nicht mehr erforderlicher Daten oder Berichtigung unrichtiger Daten nicht zu. Außerdem besteht in den USA keine unabhängige Datenschutzkontrolle. Vor diesem Hintergrund sind die im Abkommen enthaltenen weiten Öffnungsklauseln für die weitere Verwendung der ausgetauschten Daten sowie der Verzicht auf Höchstspeicherfristen aus datenschutzrechtlicher Sicht nicht akzeptabel.

20.3 Berliner Erklärung: Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts

(Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3. bis 4. April 2008)

Regelungen insbesondere zum großen Lauschangriff, zur Telekommunikationsüberwachung, zur Rasterfahndung, zur Onlinedurchsuchung, zur automatischen Auswertung von Kfz-Kennzeichen und zur Vorratsspeicherung von Telekommunikationsdaten haben die verfassungsrechtlich zwingende Balance zwischen Sicherheitsbefugnissen der staatlichen Behörden und persönlicher Freiheit der Bürgerinnen und Bürger missachtet. Das Bundesverfassungsgericht hat mit einer Reihe von grundlegenden Entscheidungen diese Balance wieder hergestellt und damit auch den Forderungen der Datenschutzbeauftragten des Bundes und der Länder größtenteils Rechnung getragen.

Die Herausforderungen für den Datenschutz gehen aber weit über die genannten Bereiche hinaus. Datenverarbeitungssysteme dringen immer stärker in alle Lebensbereiche ein und beeinflussen den Alltag. Das Internet ist zum Massenmedium geworden. Vielfältig sind dabei die Möglichkeiten, das persönliche Verhalten zu registrieren und zu bewerten. Der nächste Quantensprung der Informationstechnik steht unmittelbar bevor: die Verknüpfung von Informationstechnik mit Körperfunktionen, insbesondere bei der automatisierten Messung medizinischer Parameter und bei der Kompensation organischer Beeinträchtigungen. Die Miniaturisierung von IT-Systemen geht so weit, dass demnächst einzelne Komponenten nicht mehr mit bloßem Auge wahrgenommen werden können (Nanotechnologie).

Das Handeln staatlicher und nicht öffentlicher Stellen ist verstärkt darauf gerichtet, viele Daten ohne klare Zweckbestimmung zu sammeln, um sie anschließend vielfältig auszuwerten, beispielsweise um versteckte Risiken aufzudecken oder um persönliches Verhalten unbemerkt zu beeinflussen. Geht es der Wirtschaft etwa darum, durch Scoringverfahren die Kundinnen und Kunden vorab einzuschätzen, gewinnt die immer exzessivere Registrierung und automatisierte Beobachtung für staatliche Stellen an Bedeutung. In beiden Bereichen wird ganz normales Verhalten registriert, unabhängig von konkreten Gefahren oder Verdachtsmomenten. Auch diejenigen, die sich nichts haben zuschulden kommen lassen, werden einem verstärkten Kontroll- und Anpassungsdruck ausgesetzt, der Einschüchterungseffekte zur Folge haben wird.

Der Schutz der Grundrechte, nicht zuletzt des Datenschutzes, dient in einer demokratischen Gesellschaft auch dem Gemeinwohl und ist zunächst Aufgabe jeglicher Staatsgewalt. Darüber hinaus ist er eine gesamtgesellschaftliche Aufgabe. Schließlich ist jede Bürgerin und jeder Bürger auch zur Eigenverantwortung aufgerufen. Hilfen zum informationellen Selbstschutz müssen zur Verfügung gestellt werden, die es den Betroffenen ermöglichen, eine Erfassung ihres Verhaltens zu vermeiden und selbst darüber zu entscheiden, ob und wem gegenüber sie Daten offenbaren. Von zunehmender Bedeutung sind auch Projekte, die das Datenschutzbewusstsein fördern, um vor allem jüngere Menschen von einem fahrlässigen Umgang mit ihren persönlichen Daten abzuhalten.

Alle diese Maßnahmen tragen zur Entwicklung einer neuen Datenschutzkultur bei. Voraussetzung dafür ist auch, dass nicht länger versucht wird, die verfassungsrechtlichen Grenzen und Spielräume auszureizen. Stattdessen muss dem Gebot der Datenvermeidung und -sparsamkeit Rechnung getragen werden.

20.4 Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen

(Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3. bis 4. April 2008)

Elektronische Identitäten sind der Schlüssel zur Teilnahme an der digitalen Welt. Die Möglichkeiten der pseudonymen Nutzung, die Gewährleistung von Datensparsamkeit und -sicherheit und der Schutz vor Identitätsdiebstahl und Profilbildung sind wichtige Grundpfeiler moderner Informations- und Kommunikationstechnologien. Darauf hat die Bundesregierung zu Recht anlässlich des Zweiten Nationalen IT-Gipfels im Dezember 2007 (Hannoversche Erklärung) hingewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass der gesetzliche Rahmen für die anonyme oder pseudonyme Nutzung elektronischer Verfahren bereits seit langem vorhanden ist. Beispielsweise hat je-

der Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 13 Abs. 6 Telemediengesetz).

Bisher werden jedoch anonyme oder pseudonyme Nutzungsmöglichkeiten nur sehr selten angeboten. Vielmehr speichern Wirtschaft und Verwaltung immer mehr digitale Daten mit direktem Personenbezug. Erschlossen werden diese Datenbestände in der Regel über einheitliche Identifizierungsnummern. Mit der lebenslang geltenden bundeseinheitlichen Steuer-Identifikationsnummer (Steuer-ID) oder der mit der Planung der Gesundheitskarte zusammenhängenden, ebenfalls lebenslang geltenden Krankenversichertennummer werden derzeit solche Merkmale eingeführt. Auch mit der flächendeckenden Einführung des ePersonalausweises wird jeder Bürgerin und jedem Bürger eine elektronische Identität zugewiesen, mit der sie bzw. er sich künftig auch gegenüber E-Government-Portalen der Verwaltung oder eCommerce-Angeboten der Wirtschaft identifizieren soll.

Einheitliche Personenkennzeichen bergen erhebliche Risiken für das Recht auf informationelle Selbstbestimmung. So könnte sich aus der Steuer-ID ein Personenkennzeichen entwickeln, über das alle möglichen Datenbestände personenbezogen verknüpft und umfassende Persönlichkeitsprofile erstellt werden. Angesichts der stetig verbesserten technischen Möglichkeiten, zunächst verteilt gespeicherte Daten anwendungsübergreifend zu verknüpfen, wachsen entsprechende Begehrlichkeiten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die effektive Nutzung von Informationstechnik und hohe Datenschutzstandards keinen Widerspruch bilden. Ein datenschutzförderndes Identitätsmanagement kann den Einzelnen vor unangemessener Überwachung und Verknüpfung seiner Daten schützen und zugleich eine moderne und effektive Datenverarbeitung ermöglichen. Entsprechende EU-Projekte wie PRIME (Privacy and Identity Management for Europe) und FIDIS (Future of Identity in the Information Society) werden im Rahmen des 6. Europäischen Forschungsprogramms „Technologien für die Informationsgesellschaft“ gefördert.

Identitätsmanagement sollte auf der anonymen oder pseudonymen Nutzung von elektronischen Verfahren und der dezentralen Haltung von Identifikationsdaten unter möglichst weitgehender Kontrolle der betroffenen Bürgerinnen und Bürger basieren. Datenschutzfördernde Identitätsmanagementsysteme schließen Verknüpfungen nicht aus, wenn die Nutzenden es wünschen oder wenn dies gesetzlich vorgesehen ist. Sie verhindern jedoch, dass unkontrolliert der Bezug zwischen einer elektronischen Identität und einer Person hergestellt werden kann. Unter bestimmten, klar definierten Bedingungen kann mit Hilfe von Identitätsmanagementsystemen sichergestellt werden, dass ein Pseudonym bei Bedarf bezogen auf einen bestimmten Zweck (z. B. Besteuerung) einer Person zugeordnet werden kann.

Identitätsmanagementsysteme werden nur dann die Akzeptanz der Nutzerinnen und Nutzer finden, wenn sie einfach bedienbar sind, ihre Funktionsweise für alle Beteiligten transparent ist, möglichst alle Komponenten standardisiert sind und die Technik von unabhängigen Dritten jederzeit vollständig nachprüfbar ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung daher auf, den Absichtserklärungen des IT-Gipfels Taten folgen zu lassen und den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben. Sowohl die öffentliche Verwaltung als auch die Wirtschaft sollten die Einführung solcher datenschutzfördernder Systeme unterstützen.

20.5 Vorgaben des Bundesverfassungsgerichts bei der Onlinedurchsuchung beachten

(Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3. bis 4. April 2008)

1. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass das Bundesverfassungsgericht die Regelung zur Onlinedurchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen für nichtig erklärt hat. Hervorzuheben ist die Feststellung des Gerichts, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. 25 Jahre nach dem Volkszählungsurteil hat das Bundesverfassungsgericht damit den Datenschutz

verfassungsrechtlich weiter gestärkt und ihn an die Herausforderungen des elektronischen Zeitalters angepasst.

2. Ein solches Grundrecht nimmt auch den Staat in die Verantwortung, sich aktiv für die Vertraulichkeit und Integrität informationstechnischer Systeme einzusetzen. Das Bundesverfassungsgericht verpflichtet den Staat, im Zeitalter der elektronischen Kommunikation Vertraulichkeit zu gewährleisten. Nunmehr ist der Gesetzgeber gehalten, diesen Auftrag konsequent umzusetzen. Dazu müssen die Regelungen, welche die Bürgerinnen und Bürger vor einer „elektronischen Ausforschung" schützen sollen, gemäß den Vorgaben des Gerichts insbesondere im Hinblick auf technische Entwicklungen verbessert werden. Hiermit würde auch ein wesentlicher Beitrag geleistet, Vertrauen in die Sicherheit von E-Government- und E-Commerce-Verfahren herzustellen.

3. Die Konferenz unterstützt die Aussagen des Gerichts zum technischen Selbstschutz der Betroffenen. Ihre Möglichkeiten, sich gegen einen unzulässigen Datenzugriff zu schützen, etwa durch den Einsatz von Verschlüsselungsprogrammen, dürfen nicht unterlaufen oder eingeschränkt werden.

4. Die Konferenz begrüßt außerdem, dass das Bundesverfassungsgericht das neue Datenschutzgrundrecht mit besonders hohen verfassungsrechtlichen Hürden vor staatlichen Eingriffen schützt. Sie fordert die Gesetzgeber in Bund und Ländern auf, diese Eingriffsvoraussetzungen zu respektieren. Die Konferenz spricht sich in diesem Zusammenhang gegen Onlinedurchsuchungen durch die Nachrichtendienste aus.

5. Das Bundesverfassungsgericht hat den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung auch bei Eingriffen in informationstechnische Systeme zu gewährleisten. Unvermeidbar erhobene kernbereichsrelevante Inhalte sind unverzüglich zu löschen. Eine Weitergabe oder Verwertung dieser Inhalte ist auszuschließen.

6. Auch wenn Onlinedurchsuchungen innerhalb der durch das Bundesverfassungsgericht festgelegten Grenzen verfassungsgemäß sind, fordert die Konferenz die Gesetzgeber auf, die Erforderlichkeit von Onlinedurchsuchungsbefugnissen kritisch zu hinterfragen. Sie müssen sich die Frage stellen, ob sie den Sicherheitsbehörden entsprechende Möglichkeiten an die Hand geben wollen. Die Konferenz bezweifelt, dass dieser weiteren Einbuße an Freiheit ein adäquater Gewinn an Sicherheit gegenübersteht.

7. Sollten gleichwohl Onlinedurchsuchungen gesetzlich zugelassen werden, sind nicht nur die vom Bundesverfassungsgericht aufgestellten verfassungsrechtlichen Hürden zu beachten. Die Konferenz hält für diesen Fall zusätzliche gesetzliche Regelungen für erforderlich. Zu ihnen gehören vor allem folgende Punkte:

   — Soweit mit der Vorbereitung und Durchführung von Onlinedurchsuchungen der Schutzbereich von Art. 13 GG (Unverletzlichkeit der Wohnung) betroffen ist, bedarf es dafür jedenfalls einer besonderen Rechtsgrundlage.

   — Der vom Bundesverfassungsgericht geforderte Richtervorbehalt ist bei Onlinedurchsuchungen mindestens so auszugestalten wie bei der akustischen Wohnraumüberwachung. Ergänzend zu einer richterlichen Vorabkontrolle ist eine begleitende Kontrolle durch eine unabhängige Einrichtung vorzuschreiben.

   — Gesetzliche Regelungen, welche Onlinedurchsuchungen zulassen, sollten befristet werden und eine wissenschaftliche Evaluation der dabei gewonnenen Erkenntnisse und Erfahrungen anordnen.

   — Informationstechnische Systeme, die von zeugnisverweigerungsberechtigten Berufsgruppen genutzt werden, sind von heimlichen Onlinedurchsuchungen auszunehmen.

   — Für die Durchführung von „Quellen-Telekommunikationsüberwachungen", die mit der Infiltration von IT-Systemen einhergehen, sind die gleichen Schutzvorkehrungen zu treffen wie für die Onlinedurchsuchung selbst.

8. Schließlich sind die Gesetzgeber in Bund und Ländern aufgrund der Ausstrahlungswirkung der Entscheidung des Bundesverfassungsgerichts gehalten, die sicherheitsbehördlichen Eingriffsbefugnisse in Bezug auf informationstech-

nische Systeme, z. B. bei der Überwachung der Telekommunikation im Internet sowie der Beschlagnahme und Durchsuchung von Speichermedien, grundrechtskonform einzuschränken.

20.6 Keine Vorratsspeicherung von Flugpassagierdaten

(Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3. bis 4. April 2008)

Die EU-Kommission hat den Entwurf eines Rahmenbeschlusses des Rates zur Speicherung von Flugpassagierdaten und zu deren Weitergabe an Drittstaaten vorgelegt. Künftig sollen die Fluggesellschaften bei Flügen aus der EU und in die EU zu jedem Fluggast insgesamt 19 Datenelemente, bei unbegleiteten Minderjährigen sechs weitere Datenelemente, an eine von dem jeweiligen Mitgliedstaat bestimmte „Zentralstelle" übermitteln. Die Daten sollen bei den Zentralstellen anlass- und verdachtsunabhängig insgesamt 13 Jahre lang personenbezogen gespeichert werden und zur Durchführung von Risikoanalysen dienen. Unter im Einzelnen noch unklaren Voraussetzungen sollen die Daten an Strafverfolgungsbehörden von Nicht-EU-Staaten (z. B. die USA), übermittelt werden dürfen. Neben Grunddaten zur Person, über Reiseverlauf, Buchungs- oder Zahlungsmodalitäten und Sitzplatzinformationen sollen auch andere persönliche Angaben gespeichert werden. Unklar ist, welche Daten unter „allgemeine Hinweise" gespeichert werden dürfen. Denkbar wäre, dass beispielsweise besondere Essenswünsche erfasst werden.

Mit der beabsichtigten Vorratsspeicherung und der Datenübermittlung wird die EU es auswärtigen Staaten ermöglichen, Bewegungsbilder auch von EU-Bürgerinnen und -Bürgern zu erstellen. In Zukunft besteht die Gefahr, dass Menschen Angst haben werden, durch ihre Reisegewohnheiten aufzufallen.

Die in dem Rahmenbeschluss vorgesehene Vorratsdatenspeicherung von Daten sämtlicher Fluggäste, die EU-Grenzen überschreiten, verstößt nicht nur gegen Art. 8 der Europäischen Menschenrechtskonvention und die Europaratskonvention 108, sondern ist auch mit dem im Grundgesetz verankerten Recht auf informationelle Selbstbestimmung nicht vereinbar. Grundrechtseingriffe „ins Blaue hinein", also Maßnahmen ohne Nähe zu einer abzuwehrenden Gefahr, sind unzulässig.

Der Vorschlag für den Rahmenbeschluss erfolgte, ohne den Nutzen der erst jüngst in nationales Recht umgesetzten Richtlinie 2004/82/EG[1], die bereits alle Beförderungsunternehmen verpflichtet, die Daten von Reisenden an die Grenzkontrollbehörden zu übermitteln, auszuwerten. Hinzu kommt, dass der Vorschlag kaum datenschutzrechtliche Sicherungen enthält. Er bezieht sich nur auf eine bisher nicht bestehende und im Entwurf mit Mängeln behaftete EU-Datenschutzregelung. Diese Mängel wirken sich dadurch besonders schwerwiegend aus, dass in den Drittstaaten ein angemessenes Datenschutzniveau nicht immer gewährleistet ist und eine Änderung dieser Situation auch in Zukunft nicht zu erwarten ist.

Die EU-Kommission hat nicht dargelegt, dass vergleichbare Maßnahmen in den USA, in Kanada oder in Großbritannien einen realen, ernst zu nehmenden Beitrag zur Erhöhung der Sicherheit geleistet hätten. Sie hat die kritischen Stellungnahmen der nationalen und des Europäischen Datenschutzbeauftragten sowie der Art.-29-Datenschutzgruppe nicht berücksichtigt.

Die Konferenz fordert die Bundesregierung auf, den Entwurf abzulehnen. Sie teilt die vom Bundesrat geäußerten Bedenken an der verfassungsrechtlichen Zulässigkeit der Speicherung der Passagierdaten.

20.7 Keine Daten der Sicherheitsbehörden an Arbeitgeber zur Überprüfung von Arbeitnehmerinnen und Arbeitnehmern

(Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3. bis 4. April 2008)

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Übermittlung polizeilicher und nachrichtendienstlicher Erkenntnisse an Arbeitgeber zur Überprüfung von Bewerberinnen und Bewerbern, Beschäftigten und Fremdpersonal (z. B. Reinigungskräfte) außerhalb gesetzlicher Grundlagen. In zunehmendem Maß bitten Arbeitgeber die Betroffenen, in eine Anfrage des

1 RL 2004/82 EG v. 29.4.2004 Amtsbl. L 261 (2004) S. 24 ff., Richtlinie über die Verpflichtung von Beförderungsunternehmen, Angaben über die Beförderten zu übermitteln

Arbeitgebers bei der Polizei oder dem Verfassungsschutz zu etwaigen dort vorliegenden Erkenntnissen zu ihrer Person einzuwilligen. In anderen Fällen sollen die Betroffenen eine solche Auskunft („fremdbestimmte Selbstauskunft") selbst einholen und ihrem Arbeitgeber vorlegen. Eine solche „Einwilligung des Betroffenen" ist regelmäßig keine wirksame Einwilligung. Die Betroffenen sehen sich oftmals dem faktischen Druck des Wohlverhaltens zum Zwecke des Erhalts und der Sicherung des Arbeitsplatzes ausgesetzt.

Die gesetzliche Grundentscheidung, in einem „Führungszeugnis" dem Arbeitgeber nur ganz bestimmte justizielle Informationen zu einer Person verfügbar zu machen, wird dadurch unterlaufen. Es stellt einen Dammbruch dar, wenn jeder Arbeitgeber durch weitere Informationen direkt oder indirekt an dem Wissen der Sicherheitsbehörden und Nachrichtendienste teilhaben kann. Die Übermittlung dieser Informationen an Arbeitgeber kann auch den vom Bundesarbeitsgericht zum „Fragerecht des Arbeitgebers" getroffenen Wertentscheidungen widersprechen. Danach darf der Arbeitgeber die Arbeitnehmerinnen und Arbeitnehmer bei der Einstellung nach Vorstrafen und laufenden Ermittlungsverfahren fragen, wenn und soweit die Art des zu besetzenden Arbeitsplatzes dies erfordert.

Polizei und Nachrichtendienste speichern – neben den in ein „Führungszeugnis" aufzunehmenden Daten – auch personenbezogene Daten, die in das Bundeszentralregister gar nicht erst eingetragen werden oder Arbeitgebern in einem „Führungszeugnis" nicht übermittelt werden dürfen. Es stellt eine grundsätzlich unzulässige Durchbrechung des Zweckbindungsgrundsatzes dar, wenn ein Arbeitgeber diese Daten – über den Umweg über die Polizei oder einen Nachrichtendienst – für Zwecke der Personalverwaltung erhält. Dabei ist besonders zu beachten, dass polizeiliche oder nachrichtendienstliche Daten nicht zwingend gesicherte Erkenntnisse sein müssen, sondern oftmals lediglich Verdachtsmomente sind. Die Folgen von Missdeutungen liegen auf der Hand.

20.8 Medienkompetenz und Datenschutzbewusstsein in der jungen „Online-Generation"

(Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3. bis 4. April 2008)

1. Die Nutzung moderner Informationssysteme ist auch mit Risiken verbunden. Diese begründen ein besonderes Schutzbedürfnis der Bürgerinnen und Bürger. Dieses verlangt aber nicht nur rechtliche Vorkehrungen und Sicherungen, sondern auch Aufklärung und Information darüber, mit welchen Risiken die Nutzung dieser Informationssysteme verbunden sind. Dies gilt vor allem für die junge „Online-Generation", die in der Altersgruppe der 14- bis 19-Jährigen zu 96 % regelmäßig das Internet nutzt, und zwar im Durchschnitt länger als zweieinhalb Stunden täglich.

2. Die Datenschutzbeauftragten des Bundes und der Länder sehen es daher als wichtige Aufgabe an, Kinder und Jugendliche für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den Daten anderer zu sensibilisieren. Diese Aufgabe obliegt gesellschaftlichen Einrichtungen ebenso wie staatlichen Organen.

   Die Erfahrungen, die anlässlich des 2. Europäischen Datenschutztages am 28. Januar 2008 gemacht wurden, stützen dies. Zu dem Motto „Datenschutz macht Schule" wurde von den Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl von Veranstaltungen und Schulbesuchen organisiert. Eltern, Lehrkräfte, Schülerinnen und Schüler, aber auch Studierende hatten dabei die Möglichkeit, sich z. B. bei Podiumsdiskussionen, Rollenspielen und Workshops über datenschutzrelevante Fragen bei der Nutzung moderner Medien zu informieren. Die dabei gewonnenen Erfahrungen lassen nicht nur einen enormen Informationsbedarf, sondern auch ein großes Informationsinteresse erkennen, und zwar bei allen Beteiligten, bei den Jugendlichen ebenso wie bei ihren Eltern und den Lehrkräften.

   Bei den Informationsangeboten, die derzeit den Schulen angeboten werden, um die Medienkompetenz junger Menschen zu verbessern, spielt das Thema „Datenschutz" aber nur eine untergeordnete Rolle. Es beschränkt sich überwiegend auf Fragen der Datensicherheit und wird zudem häufig von Fragen des Jugendmedienschutzes und des Verbraucherschutzes überlagert.

3. Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für notwendig, dass die für die schulische Bildung zuständigen Ministerinnen und Minister der Landesregierungen bei der Förderung der Medienkompetenz von Kindern und Jugendlichen – schon im Grundschulalter – deren Datenschutzbewusstsein stärken. Der Datenschutz muss bei den Angeboten und Projekten zur Förderung der Medienkompetenz eine größere Rolle spielen. Die bisherigen Ansätze reichen bei weitem nicht aus. Gerade bei jungen Menschen muss das Bewusstsein über den Datenschutz als Bürgerrecht und Bestandteil unserer demokratischen Ordnung stärker gefördert werden.

20.9 Entschlossenes Handeln ist das Gebot der Stunde

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. September 2008)

Nie haben sich in der jüngeren Geschichte die Skandale um den Missbrauch privater Daten in der Wirtschaft so gehäuft wie heute und damit deutlich gemacht, dass nicht nur im Verhältnis Bürger – Staat das Grundrecht auf informationelle Selbstbestimmung bedroht ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt – zuletzt in ihrer Berliner Erklärung vom 4. April dieses Jahres – auf diese Gefahren hingewiesen, die von massenhaften Datensammlungen privater Unternehmen und ihrer unkontrollierten Nutzung ausgehen. Sie hat auch deshalb den Gesetzgeber zu einer grundlegenden Modernisierung und Verbesserung des Datenschutzrechts aufgefordert und eine neue Datenschutzkultur angemahnt.

Dass jetzt endlich im politischen und gesellschaftlichen Raum die Problematik erkannt und diskutiert wird, ist zu begrüßen. Dabei kann und darf es aber nicht bleiben, nur entschlossenes Handeln kann die Bürgerinnen und Bürger vor weiterem Missbrauch ihrer persönlichen Daten schützen und das verlorene Vertrauen wiederherstellen.

Das vom Grundgesetz garantierte Recht eines jeden, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu entscheiden, muss endlich die ihm gebührende Beachtung finden. Die Weitergabe von persönlichen Angaben zu Werbezwecken darf nur mit ausdrücklicher Einwilligung der Betroffenen zulässig sein. Daten sind mit einem Vermerk über ihre Quelle zu kennzeichnen. Der Abschluss von Verträgen darf nicht von der Einwilligung in die Datenübermittlung zu Werbezwecken abhängig gemacht werden. Verstöße gegen den Datenschutz dürfen nicht ohne Konsequenzen bleiben, sondern müssen strikt geahndet werden. Deshalb müssen die bestehenden Lücken in den Bußgeld- und Strafbestimmungen geschlossen und der Bußgeld- und Strafrahmen für Datenschutzverstöße deutlich erhöht werden. Diese Sofortmaßnahmen, die bereits Gegenstand des Spitzentreffens im Bundesministerium des Innern am 4. September 2008 waren, können vom Deutschen Bundestag noch in den bereits vorliegenden Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes aufgenommen werden.

Gesetzgeberische Maßnahmen allein helfen aber nicht weiter, wenn ihre Einhaltung nicht ausreichend kontrolliert und Verstöße nicht sanktioniert werden können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, die Datenschutzaufsichtsbehörden endlich organisatorisch, personell und finanziell in die Lage zu versetzen, ihren Beratungs- und Kontrollaufgaben flächendeckend, unabhängig und wirkungsvoll nachkommen zu können und entsprechend der EU-Datenschutzrichtlinie mit wirksamen Einwirkungsbefugnissen auszustatten, die sie bisher nicht haben.

Außerdem müssen Konzepte zur grundlegenden Modernisierung des Datenschutzes entwickelt und umgesetzt werden. Wichtige Themen sollten dabei noch in dieser Legislaturperiode angegangen werden:

— Verbesserung der Protokollierung des Datenzugriffs in automatisierten Verfahren,

— Stärkung der datenschutzrechtlichen Auskunftsrechte,

— Pflicht zur Information der betroffenen Personen und der Aufsichtsbehörden bei Datenpannen und missbräuchlicher Datennutzung,

— Gewinnabschöpfung aus unbefugtem Datenhandel,

— Einführung eines gesetzlich geregelten Datenschutzaudits, mit dem unabhängig und qualifiziert die Datenschutzkonformität von Verfahren und Produkten bestätigt wird,

— Stärkung der betrieblichen Datenschutzbeauftragten als Organ der Selbstkontrolle

— Spezialisierung der Strafverfolgungsbehörden,

— Anerkennung von Datenschutzbestimmungen als verbraucherschützende Normen.

Nur wenn jetzt den Ankündigungen Taten folgen und entschlossen gehandelt wird, können die Bürgerinnen und Bürger künftig vor Datenmissbrauch und Verletzung ihres Grundrechts auf informationelle Selbstbestimmung besser als in der Vergangenheit geschützt werden.

20.10 Adress- und Datenhandel nur mit Einwilligung der Betroffenen

(Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6. bis 7. November 2008)

Der auf dem „Datenschutzgipfel" im September 2008 gefundene Konsens, den Adress- und Datenhandel zukünftig nur auf der Grundlage einer Einwilligung zuzulassen, ist in Politik und Gesellschaft auf breite Zustimmung gestoßen. Nur eine solche Lösung respektiert das informationelle Selbstbestimmungsrecht und damit die Wahlfreiheit der Verbraucherinnen und Verbraucher. Wer davon jetzt abrücken will, verkennt die aufgrund der jüngsten Datenskandale ans Licht gekommenen Missstände, deren Ursache nicht nur in der kriminellen Energie Einzelner zu suchen ist. Um die Daten der Betroffenen tatsächlich wirksam schützen zu können, muss die Wahlmöglichkeit der Menschen von Maßnahmen flankiert werden, die die Herkunft der Daten jederzeit nachvollziehbar machten.

Die von der Werbewirtschaft gegen die Einwilligungslösung ins Feld geführten Argumente sind nicht überzeugend. Die behaupteten negativen Folgen für den Wirtschaftsstandort sind nicht zu belegen. Unabhängig davon gilt: Es gibt keine schutzwürdigen Interessen für die Beibehaltung von Geschäftsmodellen, die darauf beruhen, hinter dem Rücken und ohne Information der Betroffenen mit deren Daten Handel zu treiben. Die Einführung des Einwilligungsprinzips würde im Gegenteil zielgenaueres und wirksameres Direktmarketing erlauben. Die Bundesregierung sollte sich deshalb nicht von ihrer Absicht abbringen lassen, die beim „Datenschutzgipfel" gegebenen Zusagen zur schnellen Verbesserung des Datenschutzes einzulösen. Sie würde es sonst versäumen, die notwendigen Lehren aus den jüngsten Skandalen zu ziehen. Der Referentenentwurf des Bundesinnenministeriums zur Änderung des Bundesdatenschutzgesetzes im Bereich des Adress- und Datenhandels (Stand: 22.10.2008) zieht mit der Einwilligungslösung – bei aller Verbesserungswürdigkeit im Detail – die einzig richtige und notwendige Konsequenz aus den zahlreichen Datenskandalen und darf nicht verwässert werden.

20.11 Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten

(Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6. bis 7. November 2008)

Mit der Gesundheitsreform soll über die Einführung von Wettbewerbsmechanismen die Qualität und Effizienz der gesetzlichen Krankenkassen verbessert werden. Die Kassen sind daher bemüht und auch vom Gesetzgeber gehalten, Versicherten ein Versorgungsmanagement anzubieten. Von zentraler Bedeutung sind dabei Patientenschulungsmaßnahmen und strukturierte Behandlungsprogramme für chronisch kranke Versicherte, die jedoch lediglich Angebotscharakter haben dürfen. Ihre Teilnahme soll nach dem Willen des Gesetzgebers freiwillig sein und eine eingehende Unterrichtung voraussetzen. Diese Vorgaben werden von einzelnen Krankenkassen nicht beachtet, wenn sie versuchen, die Versicherten in ihrem Gesundheitsverhalten zu steuern und sie in bestimmte Maßnahmen und Programme zu drängen.

Um Teilnehmerinnen und Teilnehmer zu gewinnen und um Maßnahmen durchzuführen, bedienen sich die Kassen vielfach privater Dienstleister und offenbaren diesen teils höchst sensible Gesundheitsdaten ihrer Versicherten. Dies ist datenschutz-

rechtlich nach dem Sozialgesetzbuch unzulässig, wenn die Übermittlung ohne Kenntnis und vorherige Einwilligung der jeweiligen Versicherten erfolgt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält die Einhaltung insbesondere der folgenden Eckpunkte bei gesundheitlichen Steuerungsprogrammen der Krankenkassen für unerlässlich:

— Die Krankenkassen dürfen Versichertendaten nur dann zur Auswahl von Personen für besondere Gesundheitsmaßnahmen verwenden, wenn dies gesetzlich ausdrücklich vorgesehen ist. Es muss sich um valide und erforderliche Daten handeln. Mit der Auswahl darf kein privater Dienstleister beauftragt werden.

— Die erstmalige Kontaktaufnahme mit potenziell für eine Gesundheitsmaßnahme in Betracht kommenden Versicherten muss durch die Krankenkasse selbst erfolgen, auch wenn ein privater Dienstleister mit der späteren Durchführung der Gesundheitsmaßnahme beauftragt worden ist.

— Die Versicherten sind vor Übermittlung ihrer Daten umfassend zu informieren. Die Information muss auch den Umstand umfassen, dass ein privates Unternehmen mit der Durchführung betraut werden soll. Soweit die Versicherten ausdrücklich in die Teilnahme eingewilligt haben, dürfen die für die Durchführung der Maßnahme erforderlichen Daten an den Dienstleister übermittelt werden.

— Wenn Versicherte – zu welchem Zeitpunkt auch immer – eindeutig zum Ausdruck bringen, nicht an einer Maßnahme teilnehmen zu wollen oder nicht an weitergehenden Informationen, einer konkreten Anwerbung oder einer fortgesetzten Betreuung interessiert zu sein, ist dies zu respektieren. Weitere Maßnahmen (auch telefonische Überredungsversuche) sind zu unterlassen.

20.12 Gegen Blankettbefugnisse für die Software-Industrie

(Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6. bis 7. November 2008)

Gegenwärtig wird auf europäischer Ebene über Änderungen der Richtlinie zum Datenschutz in der elektronischen Kommunikation (2002/58/EG) beraten. Dabei geht es auch um die Frage, ob in Zukunft einzelfallunabhängig Verkehrsdaten zur Gewährleistung der Netz- und Informationssicherheit, also etwa zur Verfolgung von Hackerangriffen, verarbeitet werden dürfen.

Bereits auf der Grundlage der geltenden Richtlinie erlaubt § 100 Telekommunikationsgesetz den Telekommunikationsdiensteanbietern eine zielgerichtete, einzelfallbezogene Datenverarbeitung zur Fehlerbeseitigung und Missbrauchsbekämpfung. Diese Regelung hat sich in der Praxis bewährt. Es ist daher nicht erforderlich, zur Gewährleistung der Netz und Informationssicherheit einzelfallunabhängig personenbezogene Verkehrsdaten zu speichern. Die Anbieter von Telekommunikationsdiensten sind aufgefordert, ihre Systeme so sicher zu gestalten, dass Angriffe von vornherein erfolglos bleiben.

Obwohl die Europäische Kommission eine Änderung der bisherigen Rechtslage nicht für erforderlich hält, schlagen mehrere Mitgliedstaaten bei den gegenwärtigen Beratungen im Rat vor, entsprechend den Vorstellungen der Software-Industrie (Business Software Alliance) eine generelle Ermächtigung in die Richtlinie aufzunehmen, wonach „jede natürliche oder juristische Person mit einem berechtigten Interesse“ berechtigt sein soll, Verkehrsdaten zu verarbeiten, um „technische Maßnahmen zur Gewährleistung der Sicherheit eines öffentlichen Telekommunikationsdienstes, eines öffentlichen oder privaten Telekommunikationsnetzes, eines Dienstes der Informationsgesellschaft oder von Endgeräten zu deren Nutzung“ zu ergreifen. Damit wäre nicht nur der jeweilige Diensteanbieter, der Maßnahmen zum Schutz des eigenen Angebots treffen will, zur einzelfallunabhängigen Speicherung von Verkehrsdaten berechtigt, sondern praktisch jeder mit einem wirtschaftlichen Verarbeitungsinteresse, insbesondere auch die Hersteller von Sicherheitssoftware.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt eine solche zeitlich unbegrenzte und inhaltlich unbestimmte Blankettermächtigung als inakzeptabel ab. Der Hinweis auf die „Informationssicherheit“ rechtfertigt es nicht, dass Verkehrsdaten nahezu uferlos auch von Dritten verarbeitet werden. Die Bundesregierung wird aufgefordert, einer derartigen Aufweichung des Telekommunikationsgeheimnisses im Rat ihre Zustimmung zu verweigern.

20.13 Mehr Transparenz durch Informationspflichten bei Datenschutzpannen

(Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6. bis 7. November 2008)

In den letzten Monaten hat eine Reihe von gravierenden Datenschutzverstößen die Aufmerksamkeit der Öffentlichkeit und der Medien gefunden. In vielen dieser Fälle lag der Verlust oder Missbrauch personenbezogener Daten längere Zeit zurück und war der verantwortlichen Stelle bekannt, ohne dass die Betroffenen oder die zuständige Datenschutzaufsichtsbehörde hierüber informiert worden wären. Dadurch wurde ihnen die Möglichkeit genommen, Sicherheitsmaßnahmen zu ergreifen und mögliche Schäden zu begrenzen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt deswegen die Forderung, alle verantwortlichen Stellen – grundsätzlich auch alle öffentlichen Stellen – gesetzlich zu verpflichten, bei Verlust, Diebstahl oder Missbrauch personenbezogener Daten unverzüglich die hiervon betroffenen Bürgerinnen und Bürger und die zuständigen Aufsichts- oder Kontrollbehörden sowie gegebenenfalls auch die Öffentlichkeit zu unterrichten. Dies entspricht ihrer datenschutzrechtlichen Verantwortung und ermöglicht es den Betroffenen, negative Konsequenzen solcher Datenschutzpannen abzuwenden oder einzugrenzen. Hinter diesem Interesse hat der Wunsch der entsprechenden Stellen zurückzustehen, solche Vorkommnisse geheim zu halten, um keinen Imageschaden oder keine wirtschaftlichen Nachteile zu erleiden.

Etliche Staaten haben bereits entsprechende Regelungen. Eine solche Informationspflicht würde die Transparenz erhöhen und das Vertrauen der Betroffenen in eine korrekte Datenverarbeitung stärken. Darüber hinaus würde sie einen wichtigen Anstoß geben, mehr für Datenschutz und Datensicherheit zu tun.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, entsprechende umfassende Informationspflichten für Unternehmen und öffentliche Stellen im Bundesdatenschutzgesetz und den Landesdatenschutzgesetzen zu schaffen. Die übrigen aus Anlass der Datenschutzskandale in einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16.09.2008 erläuterten Forderungen zur Novellierung des Bundesdatenschutzgesetzes werden bekräftigt.

20.14 Angemessener Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in der EU dringend erforderlich

(Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6. bis 7. November 2008)

Auf europäischer Ebene ist eine Vielzahl von Vorhaben beschlossen bzw. initiiert worden, die in ihrer Gesamtheit zu erheblichen Eingriffen in die Persönlichkeitsrechte führt:

— Die Telekommunikationsunternehmen in den Mitgliedstaaten der EU sind verpflichtet, die bei der Nutzung öffentlich zugänglicher Telekommunikationsdienste anfallenden Verkehrsdaten über das Kommunikationsverhalten der Einzelnen für die Sicherheitsbehörden ohne konkreten Anlass auf Vorrat zu speichern.

— Die Pässe der Bürgerinnen und Bürger der EU-Mitgliedstaaten werden mit biometrischen Merkmalen ausgestattet.

— Fluggastdaten (PNR) werden in die USA übermittelt, um sie den dortigen Behörden zur Verfügung zu stellen. Die Nutzung von Fluggastdaten zu Strafverfolgungszwecken wird auch in der Europäischen Union vorbereitet.

— Der Vertrag von Prüm, der in den Rechtsrahmen der Union überführt wird, ermöglicht den Polizei- und Strafverfolgungsbehörden der Mitgliedstaaten einen gegenseitigen Zugriff auf Fingerabdruck-, DNA- und Kfz-Daten.

— Es soll ein Europäisches Strafregisterinformationssystem geschaffen werden, mit dem Informationen über strafrechtliche Verurteilungen zwischen den Mitgliedstaaten ausgetauscht werden können.

— Das Schengener Informationssystem wird weiter ausgebaut, u. a. durch die Speicherung von biometrischen Merkmalen. Zudem wird der Kreis der Nutzer er-

weitert um das Europäische Polizeiamt EUROPOL und die Einheit für justizielle Zusammenarbeit in der EU (EUROJUST).

— Ein europäisches Visa-Informationssystem (VIS) wird eingeführt, um den Austausch von Visa-Daten zwischen den Mitgliedstaaten zu erleichtern. Auch für EUROPOL, die Sicherheitsbehörden und die Nachrichtendienste soll dieser Datenbestand zugänglich sein.

— Das europäische Verfahren EURODAC, in dem die Fingerabdrücke von Asylbewerberinnen und Asylbewerbern gespeichert sind, soll auch von der Polizei und den Strafverfolgungsbehörden genutzt werden können.

— Der Aufgabenbereich von EUROPOL soll über die Bekämpfung der organisierten Kriminalität hinaus auch auf andere Formen der schweren Kriminalität erweitert werden. Außerdem soll EUROPOL erstmals die Befugnis erhalten, Daten auch von privaten Stellen entgegenzunehmen und Zugriff auf alle polizeilich relevanten Datenbanken in der EU bekommen.

— Der Informationsaustausch zwischen den Strafverfolgungsbehörden der EU wird entsprechend dem Rahmenbeschluss des Rates vom 18. Dezember 2006 („Schwedische Initiative") ausgebaut. Danach soll der Austausch verfügbarer Daten innerhalb der EU zu den gleichen Bedingungen erfolgen wie nach nationalem Recht.

Neben diesen Vorhaben gibt es zudem Abkommen auf bilateraler Ebene zwischen EU-Mitgliedstaaten und Drittstaaten, wie z. B. das Abkommen der Bundesrepublik Deutschland mit den Vereinigten Staaten für einen erweiterten Informationsaustausch zwischen den Sicherheitsbehörden.

Der Aufbau zentraler Datenbestände und der Ausbau der grenzüberschreitenden Datenübermittlung greifen erheblich in das Grundrecht auf informationelle Selbstbestimmung ein und führen dadurch zu Gefahren für jede Einzelne und jeden Einzelnen. Diese werden noch gesteigert durch die angestrebte Verknüpfbarkeit der bestehenden und geplanten Datenbanken.

Umso wichtiger ist deshalb ein hoher und gleichwertiger Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Europa. Dies wurde von den Datenschutzbeauftragten auf nationaler und europäischer Ebene mehrfach angemahnt. Der hierzu im Oktober 2005 vorgelegte Rahmenbeschlussvorschlag genügt diesen Anforderungen nicht (siehe dazu die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 „Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen"). Zur Wahrung des erforderlichen Gleichgewichts zwischen Freiheit und Sicherheit sollten die Parlamente und Regierungen ihre Einflussmöglichkeiten bei europäischen Vorhaben stärker nutzen und dabei auch datenschutzrechtliche Aspekte einbringen. Wie notwendig ein angemessener Datenschutz ist, hat sich beim Verfahren der Aufnahme Verdächtiger in die sogenannte EU-Terrorliste gezeigt, das durch den Europäischen Gerichtshof für rechtswidrig erklärt wurde.

Die Datenschutzbeauftragten fordern deshalb:

— Bei jeder neuen Initiative ist das Verhältnismäßigkeitsprinzip zu wahren und deren Auswirkung auf das bestehende System von Eingriffsmaßnahmen zu berücksichtigen.

— Im Hinblick auf den Kumulationseffekt sind die verschiedenen europäischen Initiativen zudem grundrechtskonform aufeinander abzustimmen. Redundanzen und Überschneidungen müssen verhindert werden.

— Ein Rechtsakt muss unverzüglich beschlossen werden, der über den Rahmenbeschlussvorschlag hinaus einen hohen und gleichwertigen Datenschutzstandard bei der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit verbindlich vorschreibt. Die gesamte nationale und grenzüberschreitende Informationsverarbeitung in diesem Bereich muss davon erfasst sein, um ein einheitliches Datenschutzniveau in den EU-Mitgliedstaaten zu gewährleisten.

— Ein unabhängiges, beratendes Datenschutzgremium sowie eine unabhängige und umfassende datenschutzrechtliche Kontrolle müssen für die polizeiliche und justizielle Zusammenarbeit eingerichtet bzw. gewährleistet werden.

20.15 Datenschutzgerechter Zugang zu Geoinformationen

(Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6. bis 7. November 2008)

Die Einführung einer einheitlichen Geodateninfrastruktur und die Veröffentlichung der staatlichen Daten eröffnen ein großes Potenzial an volkswirtschaftlichem Nutzen und ist geeignet, vielen E-Government- und E-Commerce-Anwendungen die erforderliche Infrastruktur zur Verfügung zu stellen. Als einen ersten Schritt regelt das europäische Recht mit der sogenannten INSPIRE-Richtlinie, die bis Mai 2009 in nationales Recht umgesetzt werden muss, die Bereitstellung von amtlichen Geodaten nach einheitlichen Standards für europaweite behördliche, kommerzielle und private Nutzungen.

Durch diese neue Infrastruktur werden georeferenzierbare Angaben aufgrund der Erschließungsmöglichkeit über Wohnanschriften oder Eigentümer- bzw. Standortdaten als personenbezogene Daten zur Verfügung gestellt. Diesem Umstand müssen die gesetzlichen Regelungen gerecht werden und angemessene Datenschutzregelungen enthalten.

Bei der Bereitstellung amtlicher Geodaten ist sowohl nach der europäischen Richtlinie als auch nach deutschem Verfassungsrecht der Schutz personenbezogener Daten angemessen zu gewährleisten. Der Entwurf der Bundesregierung zur Umsetzung dieser Richtlinie in einem Geodatenzugangsgesetz (BT-Drs. 16/10530) sieht eine entsprechende Anwendung der Schutzvorschriften des Umweltinformationsgesetzes vor. Im Gegensatz zum einzelfallbezogenen Zugang nach den Umweltinformationsgesetzen birgt der im Entwurf eines Geodatenzugangsgesetzes vorgesehene massenhafte Abruf solcher Daten aber ein höheres datenschutzrechtliches Gefährdungspotenzial. Der Verweis auf das Umweltinformationsgesetz ist nach Ansicht der Konferenzen der Datenschutz und der Informationsfreiheitsbeauftragten des Bundes und der Länder deshalb nicht interessengerecht. Ein Geodatenzugangsgesetz muss einen differenzierenden Ausgleich zwischen Informations und Schutzinteressen für die spezielle Problematik der Geobasis und der Geofachdaten vornehmen. Es ist insbesondere zu berücksichtigen, dass nach der INSPIRE-Richtlinie die Zugangsmöglichkeit eingeschränkt werden soll, wenn der Zugang nachteilige Auswirkungen auf die Vertraulichkeit personenbezogener Daten haben kann.

20.16 Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren

(Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6. bis 7. November 2008)

Die Bundesregierung hat am 25.06.2008 den Gesetzentwurf über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) beschlossen (BT-Drs. 16/10492). Danach haben Beschäftigte die monatliche Übermittlung ihrer Einkommensdaten an die Zentrale Speicherstelle zu dulden, obwohl zurzeit nicht verlässlich abgeschätzt werden kann, in welchem Umfang die Speicherung der Daten tatsächlich erforderlich ist. Ein großer Anteil der Betroffenen wird die dem Anwendungsbereich des ELENA-Verfahrens unterfallenden Sozialleistungen niemals oder erst zu einem erheblich späteren Zeitpunkt geltend machen. Es steht somit bereits jetzt zu vermuten, dass eine große Zahl der übermittelten Daten von der Zentralen Speicherstelle wieder zu löschen sein wird, ohne jemals für irgendein Verfahren genutzt worden zu sein.

Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb wiederholt verfassungsrechtliche Bedenken unter dem Gesichtspunkt der Verhältnismäßigkeit und speziell der Erforderlichkeit geltend gemacht und eine substantiierte Begründung gefordert. Diese ist nicht erfolgt. Bisher bestehen lediglich höchst vage Erwartungen auf langfristige Effizienzsteigerungen insbesondere der Arbeitsverwaltung. Angesichts dieser Unklarheiten verbleiben erhebliche Zweifel an der Verfassungsmäßigkeit des Gesetzes. Hinzu kommt, dass derartige umfangreiche Datensammlungen Begehrlichkeiten wecken, die Daten für andere Zwecke zu verwenden.

Für den Fall, dass diese verfassungsrechtlichen Bedenken ausgeräumt werden können, sind unter dem Gesichtspunkt des technisch-organisatorischen Datenschutzes noch folgende Verbesserungen durch den Gesetz- bzw. Verordnungsgeber erforderlich:

— Es muss sichergestellt werden (z. B. durch die Einrichtung eines Verwaltungsausschusses der Zentralen Speicherstelle), dass unter Mitwirkung von Datenschutzbeauftragten gemeinsame Grundsätze zur Wahrung des Datenschutzes und der technischen Sicherheit berücksichtigt werden.

— Für die Zentrale Speicherstelle muss ein Datenschutzbeauftragter eingesetzt werden, der dazu verpflichtet ist, regelmäßig an den Verwaltungsausschuss zu berichten.

— Schlüssel zur Ver- und Entschlüsselung der bei der Zentralen Speicherstelle gespeicherten Daten dürfen nicht in der Verfügungsgewalt der Zentralen Speicherstelle liegen. Die Ver- und Entschlüsselungskomponente muss von einer unabhängigen Treuhänderstelle verantwortet werden.

— Mittelfristig ist ein Verfahren anzustreben, das die technische Verfügungsmöglichkeit über die individuellen Daten den Betroffenen überträgt.

— Das im Rahmen der ELENA-Modellvorhaben erarbeitete differenzierte Löschungskonzept muss weiterentwickelt und umgesetzt werden.

— Für abrufende Stellen sind starke Authentisierungsverfahren vorzuschreiben, die dem Stand der Technik entsprechen und den Forderungen der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren genügen.

— Für die technischen Komponenten muss eine Zertifizierung durch eine unabhängige Prüfung vorgeschrieben werden.

20.17 Abfrage von Telekommunikationsverkehrsdaten einschränken: Gesetzgeber und Praxis müssen aus wissenschaftlichen Erkenntnissen Konsequenzen ziehen

(Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6. bis 7. November 2008)

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Auftrag des Bundesministeriums der Justiz die Nutzung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung (§§ 100 g, 100 h StPO alte Fassung) evaluiert. Die Studie geht zu Recht davon aus, dass Verkehrsdaten ein hohes Überwachungspotenzial in sich tragen und besser als andere Daten dazu geeignet sind, soziale Netzwerke nachzuweisen, Beziehungen zu identifizieren und Informationen über Individuen zu generieren. Der Studie zufolge ist die Zahl der Verkehrsdatenabfragen erheblich und kontinuierlich von 10 200 (2002) auf 40 000 Abfragen (2005) angestiegen. Zudem erfasst die Maßnahme regelmäßig auch eine Vielzahl unbescholtener Bürgerinnen und Bürger.

Das Bundesministerium der Justiz hat die Studie erst im Februar dieses Jahres und somit nach der Neuregelung der Telekommunikationsüberwachung und Einführung der Vorratsdatenspeicherung veröffentlicht. Das Gutachten liefert Erkenntnisse, deren Berücksichtigung im Gesetz vom 21. Dezember 2007 erforderlich gewesen wäre. Die Datenschutzbeauftragten des Bundes und der Länder sehen sich durch die Studie in ihrer schon früher geäußerten Kritik (vgl. ihre Entschließung vom 8./9. März 2007) bestätigt. Sie fordern den Gesetzgeber auf, die gesetzliche Regelung unter folgenden Aspekten nun zügig nachzubessern:

— Die Straftatenschwelle für Verkehrsdatenabfragen sollte insbesondere im Hinblick auf die inzwischen eingeführte Vorratsdatenspeicherung auf schwere Straftaten angehoben werden. Ein bedeutsamer Anteil der überprüften Verfahren war allenfalls der mittleren Kriminalität zuzuordnen.

— Die gesetzliche Höchstdauer der Maßnahme sollte von drei auf zwei Monate reduziert werden. Das Gutachten hat gezeigt, dass die praktischen Bedürfnisse, wie sie sich in den Aktendaten und Befragungsergebnissen äußern, dadurch vollständig abgedeckt würden.

— Für die Verkehrsdatenabfrage sollten (nach dem Vorbild der Regelungen für die akustische Wohnraumüberwachung) qualifizierte Begründungspflichten in der StPO vorgesehen werden. Dabei sollten auch die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen gesetzlich geregelt werden (z. B. Beweisverwertungsverbote). Wesentliche Kritikpunkte der Studie

waren insbesondere die lediglich formelhafte Wiedergabe des Gesetzestextes sowie die häufig wörtliche Übernahme der staatsanwaltschaftlichen Anträge in den Begründungen.

— Zur Vermeidung von Rechtsunsicherheit und zur Stärkung des Richtervorbehalts sollte in den Fällen staatsanwaltschaftlicher Eilanordnung die Verwertbarkeit der erlangten Daten davon abhängig gemacht werden, dass ein Gericht rückwirkend die formelle und materielle Rechtmäßigkeit der Maßnahme feststellt. Dem Gutachten zufolge besteht insbesondere bei den Telekommunikationsunternehmen Unsicherheit, inwieweit sie zur Herausgabe der Verkehrsdaten verpflichtet sind, wenn eine staatsanwaltschaftliche Eilanordnung nicht innerhalb der gesetzlichen Frist richterlich bestätigt wird.

— Der tatsächliche Nutzen der Vorratsdatenspeicherung für die Strafverfolgung und damit die Erforderlichkeit der Maßnahme müssen in Frage gestellt werden. Bereits bei der früheren Höchstspeicherdauer von 3 Monaten waren nach der Studie 98 % der Abfragen erfolgreich.

Auch in der praktischen Anwendung der Regelungen zur Verkehrsdatenabfrage hat die Studie Defizite deutlich gemacht. Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher auch an die Strafverfolgungsbehörden und Gerichte, aus dem Gutachten Konsequenzen zu ziehen. Besonderes Augenmerk ist vor allem auf die Prüfung der Angemessenheit der Maßnahme zu richten. Dies muss auch in substantiierten Begründungen zum Ausdruck kommen. Die gesetzlich festgeschriebenen, dem Grundrechtsschutz dienenden Benachrichtigungs-, Löschungs- und Dokumentationspflichten müssen – trotz hoher Belastungen in der Praxis – unbedingt eingehalten werden. Der Richtervorbehalt muss seine grundrechtssichernde Funktion effizient erfüllen können. Die Justizverwaltungen sind in der Verantwortung, hierfür ausreichende personelle Ressourcen zur Verfügung zu stellen.

Eine Fortführung der wissenschaftlichen Evaluation der Verkehrsdatenabfrage ist – unter den neuen rechtlichen Rahmenbedingungen und aufgrund der Weiterentwicklung der Technik – unerlässlich. Insbesondere sollten dabei Notwendigkeit und Nutzen der Verkehrsdatenabfrage – auch im Vergleich zu anderen möglichen Maßnahmen – mit Blick auf den Verhältnismäßigkeitsgrundsatz auf den Prüfstand gestellt werden.

20.18 Elektronische Steuererklärung sicher und datenschutzgerecht gestalten

(Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6. bis 7. November 2008)

Mit dem Steuerbürokratieabbaugesetz (BR-Drs. 547/08) sollen u. a. verfahrenstechnische Regelungen für die elektronische Übermittlung von Steuererklärungen durch Steuerpflichtige festgelegt werden. Zu diesem Zweck soll § 150 Abgabenordnung (AO) durch Abs. 7 Satz 1 dahingehend ergänzt werden, dass bei Einführung einer Verpflichtung zur elektronischen Abgabe die übermittelten Steuerdaten mit einer qualifizierten Signatur nach dem Signaturgesetz zu versehen sind.

Die Konferenz sieht es kritisch, dass § 150 Abs. 7 Satz 2 Nr. 6 und 7 AO auch vorsieht, zur Erleichterung und Vereinfachung des automatisierten Besteuerungsverfahrens anstelle der qualifizierten elektronischen Signatur ein sogenanntes anderes sicheres Verfahren im Benehmen mit dem Bundesinnenministerium zuzulassen oder sogar auf beide Verfahren vollständig zu verzichten. In der Gesetzesbegründung wird darauf verwiesen, dass neben der qualifizierten elektronischen Signatur künftig auch eine Übermittlung der Daten unter Nutzung der Möglichkeiten des neuen elektronischen Personalausweises möglich sein soll.

Bereits in ihrer Entschließung zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren vom 11. Oktober 2006 hat die Konferenz gefordert, Nutzenden die Möglichkeit zu eröffnen, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt daher die vorgesehene Regelung in der AO zur Nutzung der qualifizierten elektronischen Signatur, da dieses Verfahren geeignet ist, die Authentizität und Integrität eines elektronisch übermittelten Dokuments sicherzustellen und somit die handschriftliche Unterschrift ersetzen kann.

Die Datenschutzbeauftragten des Bundes und der Länder erklären hierzu:

1. Das Verfahren der qualifizierten elektronischen Signatur nach dem Signaturgesetz ist im Hinblick auf die Authentizität und Integrität elektronisch übermittelter Dokumente derzeit alternativlos.

2. Für die Bewertung anderer Verfahren sollte unmittelbar auf die Fachkenntnis unabhängiger Gutachter abgestellt werden. Als Gutachter für die Beurteilung der technischen Sicherheit kämen etwa die Bundesnetzagentur oder das BSI in Frage.

3. Steuerpflichtige müssen auch im elektronischen Besteuerungsverfahren die Möglichkeit haben, die elektronische Kommunikation mit der Finanzverwaltung durch das hierfür geeignete Verfahren der qualifizierten elektronischen Signatur abzusichern.

20.19 Besserer Datenschutz bei der Umsetzung der „Schwedischen Initiative" zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedstaaten geboten

(Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6. bis 7. November 2008)

Der Rahmenbeschluss des Rates zur Vereinfachung des Informationsaustausches zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten (sog. „Schwedische Initiative") vom 18.12.2006 verpflichtet diese, an die grenzüberschreitende Übermittlung personenbezogener Daten innerhalb der EU keine höheren Anforderungen zu stellen, als auf nationaler Ebene für den Datenaustausch zwischen Polizei und Strafverfolgungsbehörden gelten. Seine Umsetzung wird zu einem deutlichen Anstieg und zur Beschleunigung des Informationsaustausches und damit zu einer weiteren Intensivierung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen auf EU-Ebene führen. Das erstrebte Ziel, nämlich die Schaffung eines Raumes der Freiheit, der Sicherheit und des Rechts, setzt aber auch voraus, dass in den Mitgliedstaaten ein möglichst gleichwertiger Datenschutz auf hohem Niveau besteht. Dies ist bislang nicht erfüllt. Es besteht nach wie vor der aus datenschutzrechtlicher Sicht unhaltbare Zustand, dass die auf EU-Ebene ausgetauschten polizeilichen Informationen in den jeweiligen EU-Mitgliedstaaten unterschiedlichen Datenschutzregelungen hinsichtlich ihrer Verwendung unterworfen sind. Zudem gelten keine einheitlichen Rechte auf Auskunft, Berichtigung und Löschung der Datenverarbeitung für die Betroffenen in den Empfängerstaaten.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, den bei der innerstaatlichen Umsetzung der „Schwedischen Initiative" verbleibenden Spielraum zu nutzen und die Befugnisse zum Informationsaustausch mit den Strafverfolgungsbehörden der EU-Mitgliedstaaten für die nationalen Polizei und Strafverfolgungsbehörden normenklar und unter Beachtung des Grundsatzes der Verhältnismäßigkeit gesetzlich zu regeln. Dazu zählen insbesondere:

— Ausschluss der gesonderten Erhebung der angefragten Daten durch die Strafverfolgungsbehörden allein um diese zu übermitteln,

— eindeutige inhaltliche Anforderungen, die an ein Ersuchen um Datenübermittlung zu stellen sind, um Überschussinformationen zu vermeiden,

— Regelung enger Voraussetzungen für sog. Spontanübermittlungen, um für den Empfänger nutzlose und damit nicht erforderliche Übermittlungen auszuschließen,

— Nutzung des Spielraums bei der Ausgestaltung der Verweigerungsgründe, um unverhältnismäßige Datenübermittlungen zu verhindern,

— normenklare Abgrenzung der Befugnis zur Übermittlung von Daten zu präventiven Zwecken gegenüber der justiziellen Rechtshilfe,

— vollständige Umsetzung der Datenschutzbestimmungen in Art. 8 des Rahmenbeschlusses und begrenzende Regelungen zur Weiterübermittlung an Drittstaaten,

— normenklare Bestimmung, welche Behörden als zuständige Strafverfolgungsbehörden im Sinne des Rahmenbeschlusses gelten und welche Informationen nur durch Ergreifen von Zwangsmaßnahmen im Sinne des Rahmenbeschlusses verfügbar sind,

— normenklare Bestimmung, welche Informationen nicht vom Rahmenbeschluss erfasst werden, weil sie für die Strafverfolgungsbehörden nur durch das Ergreifen von Zwangsmaßnahmen verfügbar sind.

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

21.1 Internetportale zur Bewertung von Einzelpersonen

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 17./18. April 2008 in Wiesbaden)

1. Die Datenschutzaufsichtsbehörden weisen darauf hin, dass es sich bei Beurteilungen und Bewertungen von Lehrerinnen und Lehrern sowie von vergleichbaren Einzelpersonen in Internetportalen vielfach um sensible Informationen und subjektive Werturteile über Betroffene handelt, die in das Portal eingestellt werden, ohne dass die Urheber erkennbar sind und die jederzeit von jedermann abgerufen werden können.
2. Anbieter entsprechender Portale haben die Vorschriften des Bundesdatenschutzgesetzes über die geschäftsmäßige Verarbeitung personenbezogener Daten einzuhalten.
3. Bei der danach gesetzlich vorgeschriebenen Abwägung ist den schutzwürdigen Interessen der bewerteten Personen Rechnung zu tragen. Das Recht auf freie Meinungsäußerung rechtfertigt es nicht, das Recht der Bewerteten auf informationelle Selbstbestimmung generell als nachrangig einzustufen.

21.2 Datenschutzkonforme Gestaltung sozialer Netzwerke

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 17./18. April 2008 in Wiesbaden)

Der datenschutzgerechten Gestaltung sozialer Netzwerke im Internet kommt eine zentrale Bedeutung zu. Die Aufsichtsbehörden rufen in diesem Zusammenhang in Erinnerung, dass Anbieter in Deutschland zur Einhaltung des Regulierungsrahmens zum Datenschutz verpflichtet sind.

Insbesondere sind folgende rechtliche Rahmenbedingungen einzuhalten:

— Anbieter sozialer Netzwerke müssen ihre Nutzer umfassend gemäß den gesetzlichen Vorschriften über die Verarbeitung ihrer personenbezogenen Daten und ihre Wahl- und Gestaltungsmöglichkeiten unterrichten. Das betrifft auch Risiken für die Privatsphäre, die mit der Veröffentlichung von Daten in Nutzerprofilen verbunden sind. Darüber hinaus haben die Anbieter ihre Nutzer aufzuklären, wie diese mit personenbezogenen Daten Dritter zu verfahren haben.

— Die Aufsichtsbehörden weisen darauf hin, dass nach den Bestimmungen des Telemediengesetzes (TMG) eine Verwendung von personenbezogenen Nutzungsdaten für Werbezwecke nur zulässig ist, soweit die Betroffenen wirksam darin eingewilligt haben. Bei Werbemaßnahmen aufgrund von Profildaten müssen die Betroffenen nach den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) mindestens eine Widerspruchsmöglichkeit haben. Die Aufsichtsbehörden empfehlen, dass die Anbieter die Nutzer selbst darüber entscheiden lassen, ob – und wenn ja, welche – Profil- oder Nutzungsdaten zur zielgerichteten Werbung durch den Anbieter genutzt werden.

— Die Aufsichtsbehörden erinnern weiterhin daran, dass eine Speicherung von personenbezogenen Nutzungsdaten über das Ende der Verbindung hinaus ohne Einwilligung der Nutzer nur gestattet ist, soweit die Daten zu Abrechnungszwecken gegenüber dem Nutzer erforderlich sind.

— Für eine vorauseilende Speicherung von Daten über die Nutzung sozialer Netzwerke (wie auch anderer Internetdienste) für eventuelle zukünftige Strafverfolgung besteht keine Rechtsgrundlage. Sie wird insbesondere auch nicht durch die Regelungen zur Vorratsdatenspeicherung vorgeschrieben.

— Schließlich weisen die Aufsichtsbehörden darauf hin, dass das TMG die Anbieter dazu verpflichtet, das Handeln in sozialen Netzwerken anonym oder unter Pseudonym zu ermöglichen. Dies gilt unabhängig von der Frage, ob ein Nutzer sich gegenüber dem Anbieter des sozialen Netzwerks mit seinen Echtdaten identifizieren muss.

— Die Anbieter sind verpflichtet, die erforderlichen technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Sie müssen insbesondere einen systematischen oder massenhaften Export oder Download von Profildaten aus dem sozialen Netzwerk verhindern.

— Bei der datenschutzfreundlichen Gestaltung von sozialen Netzwerken kommt den Standardeinstellungen – z. B. für die Verfügbarkeit von Profildaten für Dritte – eine zentrale Bedeutung zu. Die Aufsichtsbehörden fordern die Anbieter sozialer Netzwerke auf, datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch die die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Portal an Kinder richtet. Der Zugriff durch Suchmaschinen darf jedenfalls nur vorgesehen werden, soweit der Nutzer ausdrücklich eingewilligt hat.

— Der Nutzer muss die Möglichkeit erhalten, sein Profil auf einfache Weise selbst zu löschen. Schließlich sollten die Anbieter sozialer Netzwerkdienste die Einführung von Verfallsdaten oder zumindest automatische Sperrungen erwägen, die von den Nutzern selbst festgelegt werden können.

21.3 Keine fortlaufenden Bonitätsauskünfte an den Versandhandel

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 17./18. April 2008 in Wiesbaden)

Auskunfteien dürfen Bonitätsauskünfte gemäß § 29 Absatz 2 Nr. 1 a BDSG grundsätzlich nur erteilen, wenn der Dritte, dem die Daten übermittelt werden sollen, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat.

Besteht zwischen diesem Dritten (also dem anfragenden Unternehmen) und dem Betroffenen ein Dauerschuldverhältnis, aufgrund dessen das anfragende Unternehmen während der gesamten Dauer des Bestehens ein finanzielles Ausfallrisiko trägt (z. B. Ratenzahlungskredit, Girokonto, Energielieferungs-, Telekommunikationsvertrag), so dürfen Bonitätsauskünfte nicht nur zu dem Zeitpunkt erteilt werden, zu dem der Betroffene ein solches Vertragsverhältnis beantragt hat, sondern während der gesamten Laufzeit des Vertragsverhältnisses und bis zur Erfüllung sämtlicher Pflichten des Betroffenen.

Ein Versandhandelsgeschäft stellt als solches kein Dauerschuldverhältnis dar. Die aufgrund der bisherigen Erfahrungen mit den Kunden möglicherweise bestehende Wahrscheinlichkeit und darauf gegründete Erwartung, dass der Kunde nach der ersten Bestellung wiederholt bestellen wird, und die zur Erleichterung der Bestellvorgänge möglicherweise erfolgte Einrichtung eines „Kundenkontos“ rechtfertigten es nicht, ein Versandhandelsgeschäft mit einem Dauerschuldverhältnis gleichzusetzen.

Ein berechtigtes Interesse seitens des Versandhandels gem. § 29 BDSG ist demnach nur gegeben, wenn aufgrund eines konkreten Bestellvorgangs ein finanzielles Ausfallrisiko vorliegt.

Nach Vertragsschluss sind Bonitätsauskünfte an Versandhändler dann nicht zu beanstanden, wenn ein Ratenzahlungskredit vereinbart wurde oder noch ein offener Saldo besteht. In allen anderen Fällen ist das Rechtsgeschäft nach Abwicklung des einzelnen Kaufgeschäftes für den Versandhandel abgeschlossen, ein berechtigtes Interesse an Bonitätsauskünften ist dann nicht mehr zu belegen. Damit sind Nachmeldungen oder sonstige Beauskunftungen in dieser Konstellation rechtlich unzulässig.

Hinweis:

Die Vertreter des Versandhandels und der Auskunfteien haben sich bereit erklärt, ihre Verfahren entsprechend den vorgenannten gesetzlichen Anforderungen bis spätestens Ende September 2008 umzustellen.

21.4 Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 13./14. November 2008 in Wiesbaden)

Bei digital erfassten Fotos von Gebäude- und Grundstücksansichten, die über Geokoordinaten eindeutig lokalisiert und damit einer Gebäudeadresse und dem Ge-

bäudeeigentümer sowie den Bewohnern zugeordnet werden können, handelt es sich in der Regel um personenbezogene Daten, deren Erhebung und Verarbeitung nach dem Bundesdatenschutzgesetz zu beurteilen ist. Die Erhebung, Speicherung und Bereitstellung zum Abruf ist nur zulässig, wenn nicht schutzwürdige Interessen der Betroffenen überwiegen. Bei der Beurteilung schutzwürdiger Interessen ist von Bedeutung, für welche Zwecke die Bilddaten verwendet werden können und an wen diese übermittelt bzw. wie diese veröffentlicht werden. Die obersten Aufsichtsbehörden sind sich einig, dass die Veröffentlichung von georeferenziert und systematisch bereitgestellten Bilddaten unzulässig ist, wenn hierauf Gesichter, Kraftfahrzeugkennzeichen oder Hausnummern erkennbar sind. Den betroffenen Bewohnern und Grundstückeigentümern ist zudem die Möglichkeit einzuräumen, der Veröffentlichung der sie betreffenden Bilder zu widersprechen und dadurch die Bereitstellung der Klarbilder zu unterbinden. Keine schutzwürdigen Interessen bestehen, wenn die Darstellung der Gebäude und Grundstücke so verschleiert bzw. abstrakt erfolgt, dass keine individuellen Eigenschaften mehr erkennbar sind. Um die Möglichkeit zum Widerspruch schon vor der Erhebung zu eröffnen, sollte die geplante Datenerhebung mit einem Hinweis auf die Widerspruchsmöglichkeit rechtzeitig vorher bekannt gegeben werden. Die Widerspruchsmöglichkeit muss selbstverständlich auch noch nach der Veröffentlichung bestehen.

21.5 Novellierung des Bundesdatenschutzgesetzes in den Bereichen Adressenhandel, Werbung und Datenschutzaudit

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 13./14. November 2008 in Wiesbaden)

Der Düsseldorfer Kreis begrüßt, dass die Bundesregierung durch eine Novellierung des Bundesdatenschutzgesetzes aus den jüngst bekannt gewordenen Datenschutzverstößen im Bereich der Privatwirtschaft Konsequenzen ziehen möchte. Die uneingeschränkte Streichung des Listenprivilegs und die Pflicht zur Einholung einer Einwilligung des Betroffenen bei der Übermittlung an Dritte oder bei der Nutzung für Werbezwecke für Dritte sind erforderlich, um das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger zu stärken. Hiervon wird künftig auch die Wirtschaft profitieren. Die geplanten Änderungen ermöglichen es, Werbung zielgerichteter und ohne Streuverluste vorzunehmen und unerwünschte Belästigungen zu vermeiden, sodass das Verbrauchervertrauen in die Datenverarbeitung der Wirtschaft gestärkt wird. Die vorgesehenen Regelungen zur Klarstellung, wann eine wirksame Einwilligung in die Werbenutzung vorliegt und dass diese nicht mit wichtigen vertraglichen Gegenleistungen gekoppelt werden darf, verbessern die Transparenz und die Freiwilligkeit für den Betroffenen.

Darüber hinaus hat die beim Datenschutzgipfel am 4. September 2008 eingesetzte Länderarbeitsgruppe weitere Vorschläge zur Verbesserung des Bundesdatenschutzgesetzes unterbreitet, die jedoch bisher nicht berücksichtigt wurden.

Die derzeit geplanten Vorschriften genügen nicht, um künftig im Bereich der privaten Wirtschaft ein ausreichendes Datenschutzniveau zu verwirklichen. Hierzu bedarf es zum einen einer angemessenen Ausstattung der Datenschutzaufsichtsbehörden. Es bedarf zum anderen gemäß den europarechtlichen Vorgaben wirksamer Einwirkungsbefugnisse. Hierzu gehört neben adäquaten Kontroll- und Sanktionsmitteln die Möglichkeit, bei schwerwiegenden Datenschutzverstößen die Erhebung und Verwendung personenbezogener Daten zu untersagen. Auch die Stellung der betrieblichen Datenschutzbeauftragten sollte gestärkt werden.

Die bisherigen Vorschläge des Bundesministeriums des Innern zur Einführung eines Datenschutzaudits sind nicht geeignet, den Datenschutz in der Wirtschaft zu verbessern.

22. 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.

Entschließung der Europäischen Datenschutzkonferenz:

Die Europäische Datenschutzkonferenz hat am 18. Mai 2008 die „Erklärung von Rom“ verabschiedet.

Entschließungen der Internationalen Datenschutzkonferenz:

Die 30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre hat am 17. Oktober 2008 folgende Entschließungen gefasst:

— Akkreditierungsbeschluss,

— Entschließung zum Schutz der Privatsphäre von Kindern im Internet,

— Entschließung zur Prüfung der Einrichtung eines internationalen Tages oder einer Woche für den Schutz der Privatsphäre/Datenschutz,

— Entschließung über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen und die Erarbeitung einer gemeinsamen Entschließung zur Erstellung internationaler Normen zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten,

— Entschließung über die Errichtung einer Lenkungsgruppe zur Vertretung bei Tagungen internationaler Organisationen,

— Entschließung zum Datenschutz in sozialen Netzwerkdiensten,

— Entschließung der Website-Arbeitsgruppe.

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

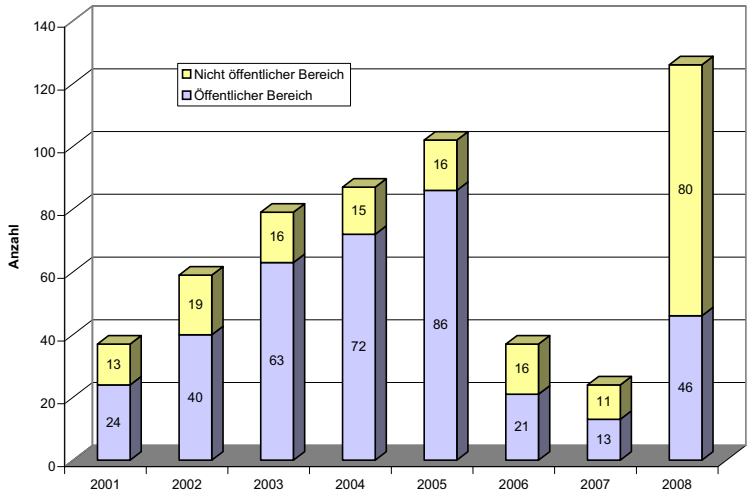
http://www.bfdi.bund.de/cln_027/nn_1208092/DE/Entschlie_C3_9Fungen/EuDSK/EUDSK__node.html__nnn=true,

http://www.bfdi.bund.de/cln_027/nn_1207974/DE/Entschlie_C3_9Fungen/IntDSK/IntDSK__node.html__nnn=true

zur Verfügung.

23. Anhang

23.1 Auswertung der Pressemitteilungen in den Jahren 2001 bis 2008



In diesem Jahr habe ich, wie auch jeweils in den letzen Jahren, eine Übersicht über die wichtigsten in der lokalen und regionalen Presse erschienen Artikel zum Datenschutz im Anhang zum Jahresbericht veröffentlicht. Die Übersicht gibt ein Stück weit Datenschutzgeschichte wie auch die Wahrnehmung des Themas in der öffentlichen Meinung wieder. Dieses Jahr habe ich mir einmal die Mühe gemacht und ein Diagramm erstellt, das zwischen Zeitungsberichten über Datenschutz im öffentlichen und im privatwirtschaftlichen Bereich differenziert. Sichtbar wird u. a., dass im Berichtsjahr dem Datenschutz in der Privatwirtschaft ein deutlich stärkeres Augenmerk gewidmet wurde, wie auch in der Tendenz – von den Jahren 2006/2007 abgesehen – eine kontinuierliche Zunahme der Berichterstattung über den Datenschutz zu vermerken ist.

23.2 Auswahl der Medienberichte in Tageszeitungen/Zeitschriften im Jahr 2008 mit Themen aus dem Land Bremen

Datum	Zeitung	Titel/Inhalt
02.01.2008	Bremer Tageszeitungen	**Verfassungsklage ohne Beispiel** Etwa 30 000 Bürger wollen Datenspeicherung kippen Der Widerstand gegen die Datenspeicherung wächst/ Ist das Privatleben in Gefahr?
04.01.2008	Nordsee-Zeitung	**Petitionen jetzt auch online**
09.01.2008	Weser-Report	**Bremer Polizeifunk live im TV** Wer in Bremen-Nord DSF guckt, hört statt „Tor, Tor, Tor“, „Inpol, bitte kommen“
13.01.2008	Kurier am Sonntag/ Delmenhorster Kreisblatt	**Bremen unter Beobachtung** Datenschützer sieht private Videoüberwachung kritisch
31.01.2008	Bremer Tageszeitungen	**Polizeigesetz zum Teil verfassungswidrig?** ADAC-Gutachter kritisiert Regelung zur Erfassung von Kennzeichen / Innenressort wartet Urteil aus Karlsruhe ab
04.03.2008	Norddeutsche	**Videoüberwachung ruft Datenschützer auf den Plan** Kameras an einer Hammersbecker Bushaltestelle sollen benachbartes Gewosie-Gebäude schützen / Behörde erscheint zum Ortstermin
10.03.2008	Bremer Tageszeitungen	**Massenkontrolle per Kamera am Straßenrand** Karlsruhe und die Angst vor dem gläsernen Autofahrer
12.03.2008	Bremer Tageszeitungen	**Erfassung von Autokennzeichen** Überprüfung der Regelung zum Kennzeichen-Scan im Bremischen Polizeigesetz
12.03.2008	Bremer Tageszeitungen	**Keiner kennt die Zahl der Videokameras** Für optisch-elektronische Überwachungsanlagen besteht keine Meldepflicht
12.03.2008	Bremer Tageszeitungen	**Rote Karte für Videoüberwachung** Karlsruhe verwarnt die Politik Datenschützer sehen in Urteil des Bundesverfassungsgerichts zur Kfz-Kontrolle Stärkung der Bürgerfreiheiten
12.03.2008	Bremer Tageszeitungen	**Ermittlung ins Blaue verboten** Karlsruhe: Massenkontrolle von Autokennzeichen verletzt den Datenschutz
12.03.2008	Weser-Report	**Kamera an die Sielwallkreuzung?** Neue „Qualität“ an Brutalität – Polizistin wurde massiv angegriffen
12.03.2008	Kreiszeitung Syke	**Innensenator will Polizeigesetz nachbessern** Bremer Datenschutzbeauftragter begrüßt Entscheidung des Bundesverfassungsgerichts zur Kennzeichenerfassung
12.03.2008	Bremer Tageszeitungen	**Bremer Gesetz auf dem Prüfstand** Überarbeitung des Bremischen Polizeigesetzes
16.03.2008	Bremer Anzeiger	**Im Gespräch mit Sven Holst** „Je weniger Überwachung, desto besser“
16.03.2008	Bremer Anzeiger	**Bald Kameras am Sielwalleck?** Überwachung geplant

Datum	Zeitung	Titel/Inhalt
23.03.2008	Bremer Tageszeitungen	**Broschüre zum Datenschutz** Herausgabe einer neuen Broschüre durch den LfDI 30.03.2008
27.03.2008	Bremer Tageszeitungen	**Big Brother bei Lidl** „stern“: Mitarbeiter mit Kameras bespitzelt/Discounter spricht von Einzelfällen
29.03.2008	Bremer Tageszeitungen	**Erst private Daten, dann das Abiturzeugnis** Landesbeauftragter legt Berichte zum Datenschutz und zur Informationsfreiheit vor / „Bedenkliche Sorglosigkeit“
29.03.2008	Nordsee-Zeitung	**Schlamperei mit den sensibelsten Daten der Bürger** Landesdatenschützer legt wieder erschreckenden Bericht vor: Arge-Mitarbeiter plappert alles am Telefon aus
30.03.2008	Bremer Anzeiger	**Holst verlangt mehr Respekt** Berichte zu Datenschutz und Informationsfreiheit
31.03.2008	taz-nord-bremen	**Polizei sieht Datenschutz locker** Laut Jahresbericht des Datenschutzbeauftragten haben sich in mindestens zwei Fällen Polizisten für private Zwecke an vertraulichen Daten vergriffen – ohne Konsequenzen für die Beamten
05.04.2008	Bremer Tageszeitungen	**Reizthema Onlinedurchsuchungen** Datenschützer sorgen sich um Balance zwischen Freiheit und Sicherheit
10.04.2008	Bremer Tageszeitungen	**Online-Netzwerke stärker im Visier von Internet-Kriminellen** Zunehmende Vernetzung der Angreifer
17.04.2008	Bremer Tageszeitungen	**Brüssel stoppt Schnüffel-Pläne** Speichern von Flug-Daten ist vom Tisch
17.04.2008	Bremer Tageszeitungen	**Rewe-Konzern gibt Überwachungen zu**
17.04.2008	Bremer Tageszeitungen	**Ersehnter Durchbruch oder ein alter Hut?** Hintergründe zu den Eckpunkten für ein Gendiagnostikgesetz, auf die sich das Kabinett geeinigt hat
20.04.2008	Bremer Anzeiger	**Schweißausbruch bei jeder E-Mail** Gefahren im Internet: „Cyberbulling“ ist weder bei Lehrern noch bei Eltern bekannt
02.05.2008	Norddeutsche	**Vorsorge für mehr Sicherheit oder Staatsspitzelei – Überwachungskameras auch in Bremen-Nord?**
04.05.2008	Kurier am Sonntag	**SCHUFA soll kostenlos Auskunft geben** Regierung will angeblich die Verbraucher bei Kreditauskünften stärken
08.05.2008	Bremer Tageszeitungen	**Datensparsamkeit ist angesagt** Sicher surfen in studiVZ & Co
15.05.2008	Bremer Tageszeitungen	**Die Rache des Ex-Freundes** Suche nach Erotikfotos im Internet
22.05.2008	Bremer Tageszeitungen	**Datenspuren verwischen** So surfen Internetnutzer anonym
22.05.2008	Bremer Tageszeitungen	**Sicherheitsbedenken beim Online-Shopping** Viele Verbraucher sehen keinen Vorteil beim Einkauf im Internet
23.05.2008	taz-nord-bremen	**Hooligan-Datei rechtswidrig** Wer im Stadion zuschlägt, landet beim BKA in der Datei „Gewalttäter Sport“

Datum	Zeitung	Titel/Inhalt
24.05.2008	Bremer Tageszeitungen	**„Überwachung bei Burger King“** Überwachung und Kontrolle der Mitarbeiter durch Videoüberwachungssystem
30.05.2008	Bremer Tageszeitungen	**RFID-Technik auf dem Vormarsch** Identifizierung erfolgt per Funk
09.06.2008	Heise online	**Bremen streicht Kfz-Kennzeichen-Scanning**
15.06.2008	Kurier am Sonntag	**Schnüffelei nach persönlichen Daten** Neue Überwachungsvorwürfe – Lufthansa unter Druck
25.06.2008	Nordsee-Zeitung	**Datenleck beim Ordnungsamt** Unbefugter greift auf Melderegister zu
28.06.2008	Bremer Tageszeitungen	**Zentrales Melderegister in Sicht** Viel Wirbel um neueste Pläne vom Bundesinnenminister Wolfgang Schäuble
28.06.2008	Bremer Tageszeitungen	**„Schäuble ist außer Rand und Band“** Sabine Leutheuser-Schnarrenberger (FDP) zu den Plänen für ein zentrales Melderegister Kommentar: Zu hohes Risiko
28.06.2008	Bremer Tageszeitungen	**Web 2.0 – Internet zum Mitmachen**
28.06.2008	Bremer Tageszeitungen	**Wenn das Netz zur Falle wird** Kinder und Jugendliche surfen zu sorglos im Internet – Wie Sprüche und Partyfotos zum „Karriere-Killer“ werden
15.07.2008	taz-nord-bremen	**Linkspartei letztmalig beobachtet** Keine Erkenntnisse
17.07.2008	Bremer Tageszeitungen	**Teilerfolg für Payback-Nutzer: Urteil stärkt Schutz von Payback-Kunden** Bundesgerichtshof: Ohne ausdrückliche Zustimmung keine Werbung per SMS oder E-Mail Kommentar: Billiger Trick
17.07.2008	taz-nord-bremen	**Payback muss Nutzer fragen** BGH-Urteil: Nur wenn Kunden einwilligen, dürfen sie elektronische Werbung bekommen
12.08.2008	Radio Bremen Nachrichten	**Holst sieht keinen Bedarf für neue Regelungen** Bremer Datenschützer zu Missbrauch von Bankdaten
13.08.2008	Bremer Tageszeitungen	**Besserer Schutz für Daten gefordert** Betrug mit Kundendaten – Moderne Art der Kaffeefahrt CD mit persönlichen Informationen von 17.000 Bürgern bei Verbraucherzentrale Schleswig-Holstein eingegangen
13.08.2008	Bremer Tageszeitungen	**Illegaler Datenhandel: Wachsamkeit ist gefragt**
14.08.2008	Bremer Tageszeitungen	**Lebenslänglich zentral erfasst** Das Bundeszentralamt für Steuern hat damit begonnen, persönliche Steuer-Identifikationsnummern zu versenden
14.08.2008	Bremer Tageszeitungen	**Vertrauen ist gut – Kontrolle ist besser** Gegen Datenmissbrauch hilft nur die eigene Vorsicht
16.08.2008	Nordsee-Zeitung	**Telefonwerber stellt sich der Polizei** Datensätze von Bürgern dreimal verkauft

Datum	Zeitung	Titel/Inhalt
17.08.2008	Sonntags-journal	**Daten-Skandal noch viel umfangreicher** Ex-Callcenter-Mitarbeiter hat 1,5 Millionen Daten gesichert
18.08.2008	Nordsee-Zeitung	**Abbuchungen niemals zugestimmt** Bremerhavenerin hätte fast 1800 Euro verloren
19.08.2008	Bremer Tageszeitungen	**Schärfere Gesetze gegen Datenklau** Kommentar: Sensibilität erhöhen
19.08.2008	Bremer Tageszeitungen	**Schwarze Schafe gibt es überall** Nicht alle Callcenter gehen verantwortungslos mit Daten um/Neues Gesetz ab 2009
20.08.2008	Burg-Lesumer Vereinsblatt	**Die eigenen Informationen schützen** LfDI: Sensible Daten nicht leichtfertig an Dritte geben
20.08.2008	Kreiszeitung Syke	**Schutz muss besser werden** Datenmissbrauch ist kein Kavaliersdelikt
20.08.2008	taz-nord-bremen	**Google kommt jetzt auch nach Bremen** Datenschützer warnt vor Angriff auf Privatsphäre – hat aber keine rechtliche Handhabe gegen den Konzern
20.08.2008	Bild-Bremen	**Internetfirma „Google“ fotografiert in Bremen**
20.08.2008	Bremer Tageszeitungen/ Delmenhorster Kreisblatt	**„Google Street View“ filmt auch in Bremen** Stadtrundfahrt mit Kamera – Datenschützer sehen keine Handhabe
20.08.2008	Nordsee-Zeitung	**„Neuer Angriff auf die Privatsphäre“** Googles „Street View“ späht Bremer aus – Datenschützer machtlos
20.08.2008	Nordsee-Zeitung	**Vivento: Kein Datenmissbrauch** „Daten für die Konkurrenz“
20.08.2008	Bremer Tageszeitungen	**„Bessere Wege für geeigneten Schutz finden“** Dieter Wiefelspütz fordert besseren Schutz vor Datenmissbrauch/Härtere Gesetze kein Allheilmittel
20.08.2008	Bremer Anzeiger	**Big Brother: Google auf Fotosafari** Seit einigen Tagen filmt der Internetkonzern die Hansestadt
21.08.2008	taz-nord-bremen	**Besserer Datenschutz** Die Bürgermeister Bremens fordern die Verbesserung des Datenschutzes
24.08.2008	Bremer Anzeiger	**Datenmissbrauch: Schärfere Gesetze und vorsichtige Bürger gefordert** Bloß nicht alles preisgeben
24.08.2008	Bremer Anzeiger	**Digitaler Datenklau ist zu einfach** Der Schutz von persönlichen Informationen verliert immer mehr an Wert
25.08.2008	taz-nord-bremen	**Musterklage gegen Steuer-ID** Derzeit erhalten alle Deutschen von der Steuerverwaltung eine Nummer, die lebenslang gilt. Bürgerrechtler klagen dagegen. Sie befürchten ein heimliches Personenkennzeichen
25.08.2008	Bremer Tageszeitungen	**Minister rangeln um Datenschutz** Uneinigkeit über die notwendigen Schritte gegen den zunehmenden Missbrauch privater Daten

Datum	Zeitung	Titel/Inhalt
26.08.2008	taz-nord-bremen	**Datenschutz befreien** Schleswig-Holsteins Datenschutzbeauftragter Weichert will seine Kollegen aus den Klauen der Politik lösen
26.08.2008	taz-nord-bremen	**Werbung an Grundschulen erlaubt** Die Bremer Bildungssenatorin verschickt Elternbriefe zur Einschulung und lässt sie sich vom Bremer Tageszeitungen bezahlen – die Zeitung darf dafür in dem Brief für ihre informativen Berichte zum Schulanfang werben
27.08.2008	Bremer Anzeiger	**Datenpanne in der Behörde** Versendung von Elternbriefen bei der Einschulung
27.08.2008	Nordsee-Zeitung	**Weitere Klagen über Callcenter**
28.08.2008	Bremer Tageszeitungen	**Gentests nur mit Einwilligung** Bundesregierung gegen erzwungene Gentests seitens der Arbeitgeber und Versicherungen
01.09.2008	Haus & Grund Mitgliedermagazin	**Datenmissbrauch konsequent bekämpfen**
07.09.2008	Kurier am Sonntag	**Amt warnt vor neuem Google-Browser Chrome**
07.09.2008	Bremer Anzeiger	**Rasend schnell und ziemlich neugierig** Google macht mit Chrome Microsofts Internet Explorer und Mozillas Firefox Konkurrenz
07.09.2008	Weser-Report	**Wird Google „das Internet?“** „Chrome“ könnte zu einem ernsthaften Konkurrenten des „Internet Explorers“ werden.
09.09.2008	Bremer Tageszeitungen	**Lidl-Bußgelder noch in dieser Woche** Datenschützer mehrerer Bundesländer wollen Bußgeldbescheide gegen den Lebensmittelkonzern erlassen
11.09.2008	Bremer Tageszeitungen	**Telekom hat mehr als nur einen Journalisten bespitzelt** Staatsanwaltschaft Bonn ermittelt gegen acht Verdächtige
11.09.2008	Bremer Tageszeitungen	**Gegen den Datenklau wehren** Verbraucher sollen Adresshändlern das Geschäft nicht so einfach machen
14.09.2008	Kurier am Sonntag	**Gastkommentar: Verunsicherung** Ein Datenschutzskandal jagt den anderen
17.09.2008	Bild-Bremen	**Braucht Bremen so einen Verbrechens-Atlas? (In London wurde eine solche Karte mit Verbrechenszahlen eingeführt – für jeden im Internet zu lesen.)** Der Innensenator arbeitet schon daran! Dann wüsste jeder, wo die Hansestadt sicher ist. Und wo nicht
20.09.2008	Bild-Bremen	**Hat Google Sie auch schon geknipst?** Kamera-Auto in ganz Bremen unterwegs. Jedes Haus wird fotografiert!
27.09.2008	taz-bremen-nord	**Mit Lifestyle gegen Daten-Piraten** (zur Veranstaltung des IFIT [Freies Institut für IT-Sicherheit Nordwest)]
01.10.2008	RB „buten un binnen“	**Schutz gegen Datenklau** Tipps des LfDI auf der Homepage

Datum	Zeitung	Titel/Inhalt
02.10.2008	Bild-Bremen	**Neue Internetseite für Datenschutz** Thema Datenmissbrauch auf der Homepage des LfDI
02.10.2008	taz-nord-bremen	**Einmal waschen und lidln, bitte** Friseur in Bremen überwacht Mitarbeiterinnen per Videokamera
06.10.2008	Radio Bremen Nachrichten	**Telekom soll Datenschutzkonzept überarbeiten** Datenschutzbeauftragter sieht Leichtfertigkeit
12.10.2008	Kurier am Sonntag	**Sicherheitsleck bei 30 Millionen Handy-Daten** Neue Panne bei der Deutschen Telekom/Bürger-Proteste gegen „Überwachungswahn“
15.10.2008	Bremer Anzeiger	**Wo Nachbarn gegen Nachbarn hetzen** Internet-Portal setzt auf Denunziantentum übelster Sorte/Zahlreiche Einträge in Bremen
15.10.2008	Nordsee-Zeitung	**Videoüberwachung auf Tankstellen** Kassierer haften für Schwarz-Tanker
16.10.2008	taz-nord-bremen	**Mittagessen mit Plastikgeld** Wegen chronischer Überfüllung werden die Kassen der Mensen auf einen digitalen Bezahlchip umgestellt
23.10.2008	Bremer Tageszeitungen	**Datenbank erfasst Sexualstraftäter**
24.10.2008	Bremer Tageszeitungen	**Entsetzen über Nackt-Scanner** EU-Kommission plant Einsatz der Geräte zur Sicherheit auf Flughäfen
27.10.2008	Bremer Tageszeitungen	**Reisepass im Altpapier entsorgt** Manche Bremer gehen mit ihren Daten sorglos um: Ganze Computer und Aktenordner landen auf der Straße
06.11.2008	Bremer Tageszeitungen	**Neue Serie: Der gläserne Internetnutzer – Nicht nur Google sammelt Daten und erstellt Persönlichkeitsprofile** Teil I: Jeder Klick hinterlässt Spuren
07.11.2008	Bremer Tageszeitungen	**Zugriff auf Daten erschwert** Verfassungsgericht begrenzt Vorratsdatenspeicherung
13.11.2008	Bremer Tageszeitungen	**Bundestag stimmt für BKA-Gesetz** Das letzte Wort hat Karlsruhe Opposition will das neue BKA-Gesetz wieder kippen – Regierung bleibt gelassen Kommentar: Augenmaß ist gefragt!
14.11.2008	Bremer Tageszeitungen	**Telekom bespitzelt ver.di-Chef Birske**
22.11.2008	Bremer Tageszeitungen	**Skepsis gegen BKA-Gesetz** Bürgermeister Böhrnsen will Informantenschutz weiter fassen
22.11.2008	Bremer Tageszeitungen	**Nachweis soll nicht der Kunde führen** Bankkunden sollen bei Falschberatung besser gestellt werden
25.11.2008	Bremer Tageszeitungen	**Gute Sicht vom Baugerüst auf Akten** Bürger sieht Datenvertraulichkeit nicht gewährleistet
27.11.2008	Bremer Tageszeitungen	**Vor allem Xing und Wikipedia** Studenten kommunizieren online mit Kommilitonen

Datum	Zeitung	Titel/Inhalt
08.12.2008	Bremer Tageszeitungen	**Bankdaten zum Kauf angeboten** Laut Medienbericht sind 21 Millionen Kontoverbindungen illegal im Umlauf
11.12.2008	Bremer Tageszeitungen	**Kundendaten werden besser geschützt** Weitergabe nur mit Zustimmung/Viele Ausnahmen Kommentar: Nicht nur Placebos
14.12.2008	Kurier am Sonntag	**Kontendaten-Klau ohne Folgen** Polizei gibt Entwarnung/Datenschützer fordern aber Konsequenzen
15.12.2008	Bremer Tageszeitungen	**Datenklau: Auch PIN gefunden** Kommentar: Fahrlässigkeit
17.12.2008	Bremer Tageszeitungen	**Datenspeicherung von EU-Bürgern unzulässig** Europäischer Gerichtshof: Ausländerzentralregister muss teilweise anonymisiert werden Kommentar: Klares Stopp-Signal
17.12.2008	Weser-Report	**Pleitiers am Online-Pranger** Detaillierte Konkursdaten im Internet/Kritik seitens des Datenschutzbeauftragten
18.12.2008	Bremer Tageszeitungen	**Weg ist frei für BKA-Gesetz**
20.12.2008	Bremer Tageszeitungen	**Stollen-Diebe lösen Datenskandal aus**

Bremer Tageszeitungen = Weser-Kurier und Bremer Nachrichten

23.3 Auswahl telefonischer Anfragen

Auch in diesem Jahr füge ich wieder eine Auswahl telefonisch beantworteter Anfragen bei, um die Vielfalt der Bürgeranliegen zu dokumentieren. Ich habe sie ein wenig thematisch gegliedert, um so auch Schwerpunkte unserer Beratungen deutlich zu machen. Eine Auflistung aller Anfragen würde den Rahmen des Berichts jedoch sprengen. Für die, die interessiert sind, halte ich ein umfassenderes Dokument bereit.

Thema	Antragsteller/-in
Video, Webcam, Bildkopien, Internet	
Fragen zur Videoüberwachung (Seminararbeit)	Schülerin (Kippenberg-G.)
Videoüberwachung einer Kantine und des Umkleidebereichs der Kantinenbeschäftigten	Beschäftigte, Gäste
Videoüberwachung in einem Keller durch einen Nachbarn	Hausbewohner etc.
Videoüberwachung in einem Fußballstadion durch die Polizei von Fußballspielen	Zuschauer und Gäste
Veröffentlichung von Daten- und Bildmaterial im Internet	Betroffene
Widerspruch gegen die Veröffentlichung von Fotos auf einer schuleigenen Homepage	Lehrer
Prangerwirkung im Internet	Journalist
Unzulässige Erhebung von Daten im Internet	Bürger
Videoüberwachung im Straßenraum	Autofahrer
Veröffentlichung von Fotos über Jugendliche auf der Homepage einer Kultureinrichtung	Jugendliche
Videoüberwachung in Einzelhandelsgeschäften	Kunden, Beschäftigte

Thema	Antragsteller/-in
Krankenhaus stellt Fotos und Namen von Babys ins Internet	Bürgerin
Veröffentlichung von Jahresbericht durch Sozialarbeiter im Internet	Sozialarbeiter
Filmen des Gartens und der Bewohner vom Nachbargrundstück aus	Nachbarn bzw. Wohnungsinhaber
Wie kommt die Suchmaschine Google zu meinen Daten	Betroffener
Fragen zu schüler-VZ	Mutter
Anfertigung und Einstellung von Fotos der Beschäftigten auf die Homepage des Arbeitgebers	Beschäftigte
Veröffentlichung von Fotos Beschäftigter auf der firmeneigenen Homepage	Beschäftigte
Erhebung personenbezogener Daten durch Hotel im Wege der Internetrecherche	Bürgerin
Woher bekommen Betrüger im Internet meine Daten	Bürger
. . .	**Summe 81**

BAgIS, ARGE

Datenübermittlung von der BAgIs an das Jugendamt	BAgIS-Teamleiterin
Datenübermittlung von einem Beschäftigungsträger an die BAgIS	Mitarbeiterin Beschäftigungsträger
Übermittlung von Daten einer Schule an die BAgIS	Bürger
Terminvergabe der ARGE über ein Callcenter	Mitarbeiterin Verein Solidarische Hilfe e.V.
Weitergabe von Gesundheitsdaten durch Beschäftigungsträgeran die BAgIS	Arzt
Übermittlung von Sozialdaten durch die BAgIS an die Staatsanwaltschaft	BAgIS-Teamleiterin
Hinzuziehen einer Psychologin zum Termin bei der BAgIS	Hilfeempfänger
Erhebung von Daten aus Kontoauszügen durch die BAgIS	Alg-II-Empfängerin
Hausbesuch durch die BAgIS	Hilfeempfängerin
Datenübermittlung eines Vermieters an die ARGE	Betreuer eines Hilfeempfängers
Datenerhebung bei der swb durch die BAgIS	Hilfeempfänger
Absenderstempel auf Briefen der ARGE	Hilfeempfänger
. . .	**Summe 54**

Heilberufe und Pflege

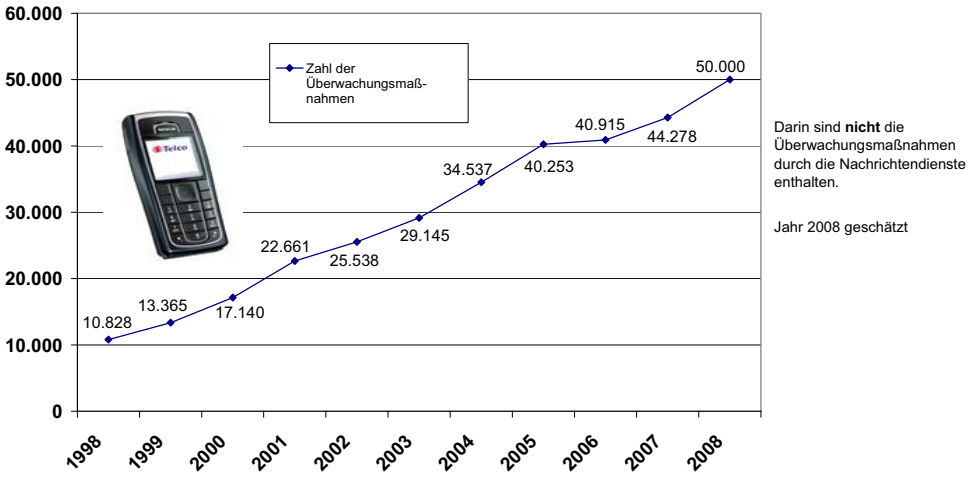
Datenaustausch zwischen Ärzten und der Krankenkasse	Bürgerin
Zugangskontrolle am PC im Pflegeheim	Mitarbeiterin Bremer Heimstiftung
Speicherung von Daten zur Medikation in einer Apotheke	Bürger
Nutzung von Diagnosedaten zur Beratungszwecken durch Krankenkassen	Arzt
Datenerhebungsbogen beim Zahnarzt	Patientin

Thema	Antragsteller/-in
Weitergabe von Daten eines Auftragnehmers bei Auftragsdatenverarbeitung im Sanitätshaus	Mitarbeiter Sanitätshaus
Akteneinsicht in Patientenakte	Patientin
Datenübermittlung durch eine Haushaltshilfe an die Krankenkasse und das Jugendamt	Bürgerin
Akustische Überwachung von Bewohnern einer Pflegeeinrichtung	Mitarbeiterin Pflegeeinrichtung
Berichtspflicht an Hausarzt bei bestimmten Verschreibungen	Gynäkologe
Einladungswesen Mammographie-Screening	Bürgerin
. . .	**Summe 56**
Hauseigentum und Miete	
Selbstauskunftsbogen eines Vermieters	Bürger
Datenerhebung zur Erstellung eines Energieausweises	Mieter
Automatisierter Datenabruf durch die Wohngeldstelle	Mitarbeiter Wohngeldstelle
Namensweitergabe durch Behörde in baurechtlichem Nachbarstreit	Bürger
. . .	**Summe 21**
Glücksspiel	
Verarbeitung psb. Daten nach Teilnahme an einer Lotterie	Bürgerin
Erforderlichkeit von Bankverbindungsdaten bei der LottoCard	Totospieler
LottoCard und Datenskandale	Bürger
Datenmissbrauch durch Internet-Gewinnspielanbieter	Bürger
Telefonwerbung vom Lottoteam, Abbuchung und Mahnverfahren	Bürgerin
Unerwünschte Telefon- und Postwerbung durch Gewinnspielunternehmen	Bürger
. . .	**Summe 33**
Beauftragte für den Datenschutz	
Fragen zur Führung von Verfahrensverzeichnissen	Datenschutzbeauftragter
Kann ein Betriebsrat die Aufgabe des Datenschutzbeauftragten wahrnehmen?	Betriebsrat
Fragen zur Bestellung von betrieblichen Datenschutzbeauftragten	Personalrat
Aufgabe des Datenschutzbeauftragten und Kontrolle des Betriebsarztes	Betrieb
. . .	**Summe 13**
Beschäftigten-Datenschutz	
Auskunft über die bei einem Rentenversicherungsträger gespeicherten Daten	Bürgerin
BSAG-Einzelfahrtennachweis für den Arbeitgeber	Beschäftigter bzw. ÖPNV-Nutzer

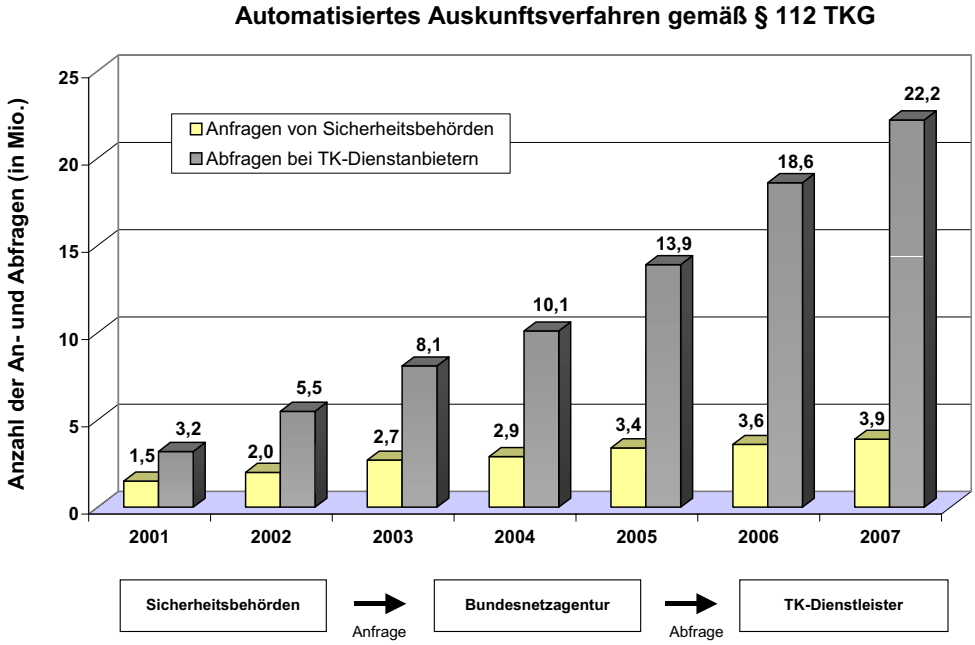
Thema	Antragsteller/-in
Einsichtnahme des Vorgesetzten in den E-Mail-Kalender des Mitarbeiters	Mitarbeiter
Bestätigung über die Löschung elektronischer Bewerberdaten	Bewerber
Datensicherung bei der Verarbeitung von Personaldaten	Beschäftigte
Speicherung von Kompetenzdaten über potenzielle Schulleiter	Lehrer
Verarbeitung von Beschäftigtendaten zur Alarmschaltung	Beschäftigte
Datenübermittlung durch Fortbildungsträger an potenzielle Arbeitgeber	Teilnehmerin
. . .	**Summe 46**
Telekommunikation	
Welche Daten darf ein Handyverkäufer erheben	Bürger
Abhören des Telefons durch Nachbarn	Bürger
Telefonanrufe nach Teilnahme an Preisausschreiben	Bürgerin
Unerwünschte Telefon- und Postwerbung durch Gewinnspielunternehmen	Bürger
Datenschutz bei einem TK-Unternehmen	Bürgerin
. . .	**Summe 27**
Polizei	
Herausgabe von IP-Adressen eines brem. Internetforums an die Polizei	Rechtsanwalt
Weitergabe eines Namens im Rahmen einer Vernehmung durch die Polizei	Bürger
ISA-Web-Auskunft Polizei Bremerhaven	Bürger
ISA-Web-Auskunft Polizei Bremen	Bürger
Lichtbild von Meldebehörde an Polizei, BKA	Bürgerin, vertreten durch Rechtsanwalt
. . .	**Summe 26**
Auskunfteien, Kreditwirtschaft	
Akteneinsicht bei der Stadtkasse, Telefongesprächsaufzeichnung bei Telefonbanking	Zahlungspflichtiger, Bankkunde
Sperrung von Daten bei einer Auskunftei	Schuldner
Abfrage der Bonität bei Auskunftei und Weiterleitung der Auskunft an Dritte	Freiberufler
. . .	**Summe 26**
Verschiedenes	
Zweckbindung von Protokollierungsdaten	zugriffsberechtigte Beschäftigte
Datenübermittlung an das Ausgleichsamt	Amtsvormund
Aufbewahrung von Akten bei einem Integrationsfachdienst	Integrationsfachdienst
Datenerhebung bei Abokündigung	Bürgerin

Thema	Antragsteller/-in
Akteneinsicht und Anfertigung von Kopien in einer Unterhaltsvorschussangelegenheit	Bürger
Umgang mit Daten von verstorbenen Vereinsmitgliedern	Bürger
Öffnen des PC bei Abwesenheit des Nutzers	Beschäftigte
Weitergabe von Schülerdaten bei Vergleichsarbeiten	Schülerinnen und Schüler
Beauftragung von Callcentern zur Datenverarbeitung durch Sozialleistungsträger	Bürgerin
Beratungsgeheimnis zwischen den Mitarbeitern einer Drogenberatungsstelle	Mitarbeiterin Drogenberatungsstelle
Gruppenauskünfte aus dem Einwohnermelderegister	Bürger
Veröffentlichung von Abgeordnetengehältern	Abgeordneter
Adressenverwendung bei Markt- und Meinungsforschung	Bürgerin
Einmeldung und Löschung von Daten des Hinweis- und Informationssystem der Versicherungswirtschaft	Versicherter
Vernichtung von Unterlagen durch Inkassounternehmen	Bürger
Auslesen von Notebooks bei Einreise in die USA	Bürgerin
Wie muss eine Rechtsanwältin und Notarin ihre Verfahrensverzeichnisse gestalten	Rechtsanwältin und Notarin
Veröffentlichung von Name und Geburtsdatum im Informationsblatt einer Kirche	Mitglied der Freikirche
Datenabfrage vom indonesischen Konsulat	Ehegatte
Weitergabe des Namens eines Informanten an einen Dritten bei Verstoß gegen das Nichtraucherschutzgesetz	Informant
Weitergabe von Forschungsdaten durch das Max-Planck-Institut	Mitarbeiter
. . .	**Summe 163**
	Gesamt 546

23.4 Anstieg der Telefonüberwachung

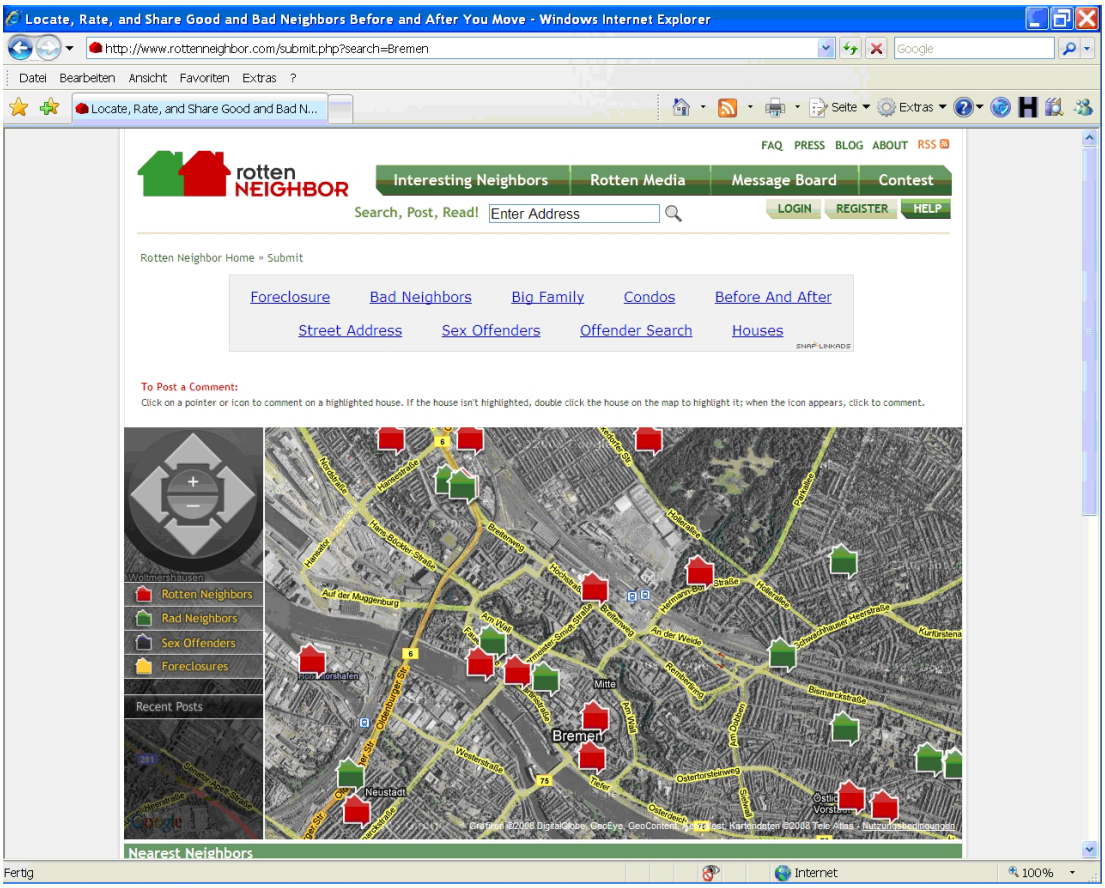


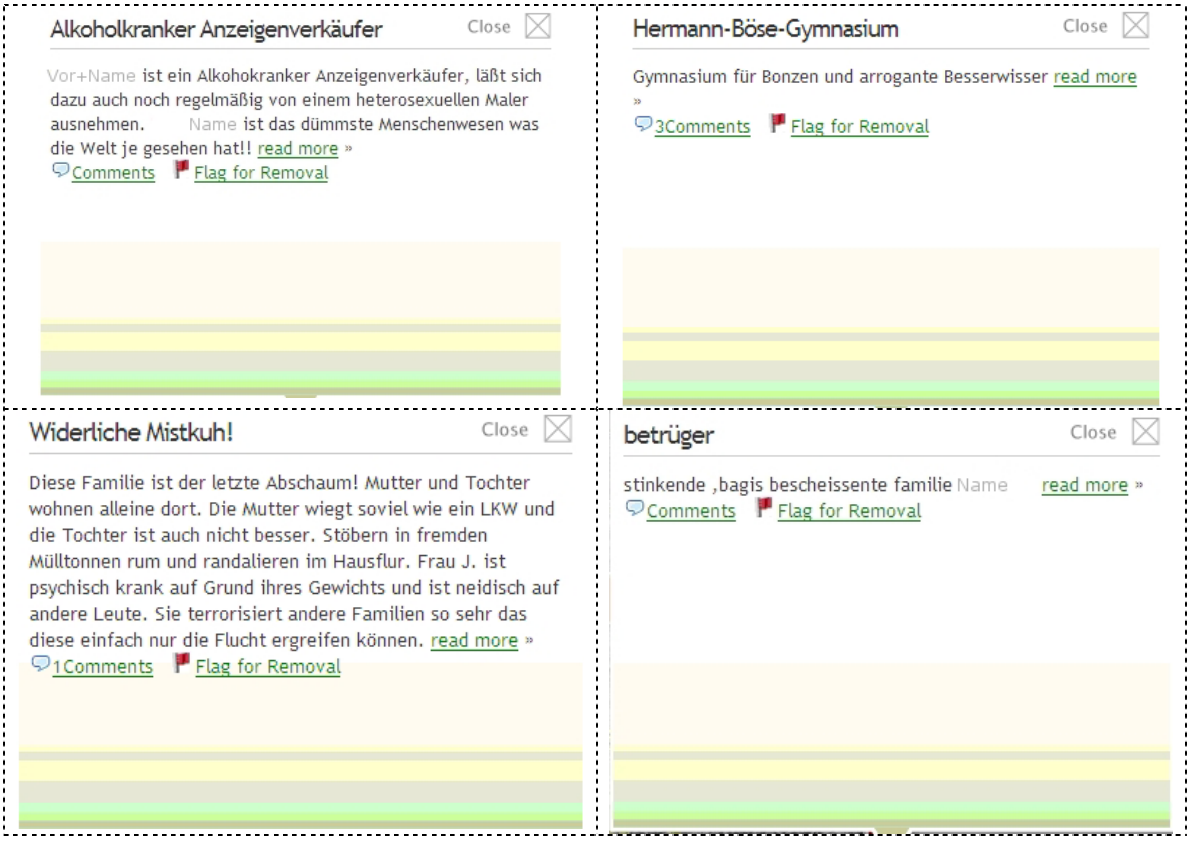
Die aktuellen Zahlen der tatsächlich in 2008 durchgeführten Maßnahmen der Telefonüberwachung liegen noch nicht vor.



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 2007 dargestellt.

23.5 Internetportal „Rotton Neighbor“





23.6 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 - 1 84 95

E-Mail: office@datenschutz.bremen.de

angefordert werden:

27. Jahresbericht 2003, Bürgerschafts-Drs. 16/578		(Restexemplare)
28. Jahresbericht 2004, Bürgerschafts-Drs. 16/980		(Restexemplare)
29. Jahresbericht 2005, Bürgerschafts-Drs. 16/1362		(Restexemplare)
30. Jahresbericht 2006, Bürgerschafts-Drs. 17/325		(Restexemplare)
Broschüre	„Datenschutz und Informationsfreiheit“	
Faltblatt	„Das Informationsfreiheitsgesetz des Bundes“	
Faltblatt	„Datenschutz bei der Polizei“	
Faltblatt	„Datenschutz im Verein“	
Faltblatt	„Adressenhandel und unerwünschte Werbung“	
Faltblatt	„Handels- und Wirtschaftsauskunfteien“	
Faltblatt	„Datenschutz bei der Internet-Telefonie“	
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.

23.7 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 Fremdwörter (z. B. AOK ...).

Abkürzung	Erklärung
Active Directory	Verzeichnisdienst
Administrator	Verwalter von Computersystemen und -netzwerken
Annexkompetenzen	Erweiterte Zuständigkeiten
AOK	Allgemeine Ortskrankenkasse
ARGE	Arbeitsgemeinschaft nach § 44 b SGB II (Sozialgesetzbuch)
Art.-29-Gruppe	Unabhängiges Beratungsgremium der Europäischen Union in Datenschutzfragen
Authentifizierung	Ausweisen für einen berechtigten Zugriff
BAgIS	Bremer Arbeitsgemeinschaft für Integration und Soziales

Abkürzung	Erklärung
BDSG	Bundesdatenschutzgesetz
Biometrie	Mess- und Auswerteverfahren an Lebewesen; eingesetzt zur Identifizierung von Individuen
BKA	Bundeskriminalamt
Blog	Abkürzung für „Weblog“; auf einer Website geführtes Tagebuch oder Journal mit chronologisch aufgeführten Einträgen
Bonität	IT-Verfahren zur IT-unterstützten Auswertung entgegengenommener Verpflichtungserklärungen
BREKOM	Bremer Kommunikationstechnik GmbH
BremIFG	Bremer Informationsfreiheitsgesetz
Browser	Computerprogramm zum Betrachten von Webseiten
Bündnis 90/Die Grünen	Politische Partei in Deutschland
BVN	Bremer Verwaltungsnetz
CD	Compact Disc; optisches Speichermedium
CDU	Christlich Demokratische Union Deutschlands (Partei)
Cookie	Kleine Datei, die von einem Webserver auf dem lokalen Computer eines Internetsurfers abgelegt wird. Sie dient u. a. der Identifizierung von Nutzern der Internetseiten.
Dataport	Dienstleister für Informations- und Kommunikationstechnik der öffentlichen Verwaltung in Schleswig-Holstein, Hamburg und Bremen sowie (teilweise) in Mecklenburg-Vorpommern
Datenschutzaudit	Überprüfung und Bewertung zur Verbesserung des Datenschutzes und der Datensicherheit von Produkten oder Verfahren
Discomeile	Gebietsabschnitt in Bremen, der bestimmte Straßenabschnitte in der Innenstadt umfasst
DNA	„Desoxyribonukleinsäure“; in allen Lebewesen vorkommendes Molekül; Träger der Erbinformation
Downloads	Umgangssprachliche Bezeichnung für aus dem Internet heruntergeladene Dateien oder Programme
DSL	„Digital Subscriber Line“, digitaler Teilnehmeranschluss mit hoher Übertragungsgeschwindigkeit zur Anbindung an das Internet
DV	Datenverarbeitung
DVD	Digital Versatile Disc; digitales, optisches Speichermedium ähnlicher der CD, aber mit höherer Speicherkapazität
eBay	Internetauktionshaus
E-Business	Integrierte Ausführung aller automatisierten Geschäftsprozesse mit Hilfe von Informationstechnologie
EDV	Elektronische Datenverarbeitung
E-Government	Elektronische Verwaltungsanwendungen, meistens Internet-basiert
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
E-Mail	Elektronische Post
ePayment	Systeme und Verfahren, um auf elektronischem Wege zu zahlen

Abkürzung	Erklärung
Erfa-Kreis	Regionaler Erfahrungsaustauschkreis der Gesellschaft für Datenschutz und Datensicherung e. V. in dem über Datenschutz- und Datensicherungsprobleme diskutiert wird
EURODAC	Europäische Datenbank zur Speicherung von Fingerabdrücken
EUROPOL	Europäische Polizeibehörde
Exchange-Server	Eigentlich „Microsoft Exchange-Server"; Groupware und Nachrichtensystem, Mail-Server
FDP	Freie Demokratische Partei Deutschlands
Firewall	System zur kontrollierten, regelbasierten Verbindung von zwei Computernetzwerken, z. B. Firmennetz und Internet
Flatrate	Pauschaltarif im Bereich der Telefon- oder Internetanbindung
GDD	Gesellschaft für Datenschutz und Datensicherung e. V.
Google	Internetsuchmaschine
Google Analytics	Kostenloser Dienst zur Analyse der Zugriffe auf Web-Seiten
Google Earth	Virtueller Globus bestehend aus Satellitenbildern
Hacking	Tätigkeit eines Hackers (Person die auf elektronischem Weg in fremde Computernetzwerke eindringt)
HEADS	Haft-Entlassenen-Auskunfts-Datei-Sexualstraftäter
Homepage	Eingang- und Eröffnungsseite einer Internetadresse
ID-Management	Zielgerichteter und bewusster Umgang mit (elektronischen) Identitäten
INSPIRE	Richtlinie zur Geodateninfrastruktur
Internetsurfer	Umgangsprachliche Bezeichnung eines Betrachters von Internetseiten
IP-Adresse	Internet-Protocol-Adresse; dient zur eindeutigen Adressierung von Computern in Netzwerken, u. a. dem Internet
ISA-Web	Informationssystem Suchen und Anzeigen im Polizeinetz
IT	Informationstechnologie
Konvergenz	Zusammenwachsen oder Annäherung von Diensten und Inhalten im Bereich der Informationstechnologie und ihrer Nutzung
KpS	Kriminalpolizeiliche Sammlung
LfV	Landesamt für Verfassungsschutz
LKA	Landeskriminalamt
Log	Protokoll in Computersystemen
Mammographie-Screening	Reihenuntersuchung der Brust bei Frauen zwischen 50 und 69 Jahren
Migrationstool	Software-Werkzeug zur Unterstützung bei der Umstellung auf neue Systeme
MiniSD-Karte	Digitales Speichermedium eines bestimmten Formats, wird z. B. in der Digital-Fotografie eingesetzt
Notebook	Tragbarer Computer, der (zeitweise) unabhängig vom Stromnetz genutzt werden kann
Onlineeinkauf	Einkauf von Waren oder Dienstleistungen auf speziellen Webseiten im Internet

Abkürzung	Erklärung
Onlineshops	Spezielle Webseite zum Handel mit Waren oder Dienstleistungen
Outsourcing	Auslagerung bestimmter Bereiche oder Aufgaben von Unternehmen an Drittunternehmen
Passwort	Kennwort, Codewort
Payback	Bestimmtes Kundenkartensystem, Kundenbindungssystem
PC	Personalcomputer
Petent	Bürger, der eine Beschwerde einlegt
PIER	Polizeiliche Information Ermittlung Recherche
PIN	Persönliche Identifikationsnummer
PNR	Passenger Name Record; Passagierregister
Portal	Spezielle Webseite, auf denen verschiedene, miteinander artverwandte Anwendungen oder Dienste zusammengefasst sind
PRIME	Name eines EU-Projektes das sich mit Datenschutz- und Identitätsmanagement befasst
Proxy-Server	Vermittler zwischen zwei Computernetzwerken
RFID	Funkchip
Roll-out	Einführung, Markteinführung
Router	Gerät im Bereich der Computernetzwerke, die mehrere dieser Netze miteinander verbinden und die Datenflüsse zwischen diesen Netzen steuern
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
Scoring	Nutzung analytisch statistischer Verfahren für Risikoabschätzungen
Security-Kit	Spezielle Option für Hard- oder Software, die ein bestehendes System um Datensicherungsfunktionen ergänzt
SIM-Karte	Chipkarte, die in einem Mobiltelefon betrieben wird und der Identifizierung des Nutzers gegenüber dem Netzbetreiber dient
Skill-Datenbank	Sammlung personenbezogener Mitarbeiterdaten zu Wissen und Fertigkeiten
SMS	Short Message Service; Telekommunikationsdienst zur Übertragung von Textnachrichten
Soziodemographisch	Begriff aus der Sozialforschung, beschreibt Bevölkerungsmerkmale
SPD	Sozialdemokratische Partei Deutschlands
StPO	Strafprozessordnung
Tool	Umgangssprachliche Bezeichnung für eine Software, die bei einer bestimmten, kleinen Aufgabe hilft, z. B. Tool zur Komprimierung von Dateien
TÜPFO	Schreibsoftware, eingesetzt in der Telekommunikationsüberwachung
Update	Aktualisierung
USB-Stick	Chipbasiertes Speichermedium zum Anschluss an DV-Systeme
User-Helpdesk	Dienst, der der Unterstützung von Anwendern von Hard- und Software dient

Abkürzung	Erklärung
Verfahrensverzeichnis	Übersicht über Angaben zur Verfahren automatisierter Verarbeitung, die von den verantwortlichen Stellen zu führen sind
ViCLAS	Bundesweite Datenbank und dient der Abbildung von Straftaten und Täterverhalten im Bereich der sexuell motivierten Gewaltkriminalität, d. h. Sexual- und Tötungsdelikte
Virtuelle Poststelle	Kryptografische Basiskomponente, mit der eine sichere und rechtsverbindliche Kommunikation realisiert werden kann; möglich wird dies durch Verschlüsselung von Nachrichten und deren Signatur (elektronische Unterschrift)
VoIP	Voice over IP; Telefonieren über Computernetzwerke, die nach Internetstandards aufgebaut sind
VwVfG	Verwaltungsverfahrensgesetz
Web 2.0	Begriff, der die veränderte Art der Nutzung und der Wahrnehmung des Internets beschreibt, bei dem die Inhalte von den Nutzern erstellt und bearbeitet werden
Webcrawler	Computerprogramm, das automatisch das Internet durchsucht und analysiert; wird meist von Internetsuchmaschinen zur Indizierung von Webseiten eingesetzt
WLAN	Wireless LAN; Standard zur Vernetzung von Computern mittels Funk
Xpider	Spezieller Webcrawler, der vom Bundesfinanzministerium betrieben wird, um Onlineverkäufern auf die Spur zu kommen, die Steuern hinterziehen könnten
ZAKS	Zentrale Antikorruptionsstelle
ZAUBER	Bundesweite Datenbank im Bereich der Finanzverwaltung. Umfasst Steuerdaten, unterliegt dem Steuergeheimnis und dient der Bekämpfung von Umsatzsteuerbetrug und der Sicherung des Umsatzsteueraufkommens

23.8 Index

Druck: Anker-Druck Bremen