27. Jahresbericht

des Landesbeauftragten für den Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats über das Ergebnis der Tätigkeit im Jahre 2004 den 27. Jahresbericht zum 31. März 2005 (§ 33 Abs. 1 Bremisches Datenschutzgesetz – BremDSG). Redaktionsschluss für die Beiträge war der 31. Dezember 2004.

Sven Holst

Landesbeauftragter für den Datenschutz

Inhaltsverzeichnis

1. Vorwort

Der Schwerpunkt meines Jahresberichts liegt auf dem Datenschutz im Land Bremen. Gleichwohl nehme ich wie in jedem Jahre im Vorwort die Gelegenheit wahr, über technische und gesellschaftliche Entwicklungen zu berichten, die zwar nicht in Bremen entstanden sind, die aber das Recht auf informationelle Selbstbestimmung tangieren und deren Auswirkungen auch die Bremer Bürgerinnen und Bürger zu spüren bekommen. Rückblickend betrachtet lässt sich die eine oder andere Entwicklung im Lande so besser einordnen.

Dies gilt z. B. auch für das wohl herausragendste datenschutzrechtliche Ereignis des vergangenen Jahres, das Urteil des Bundesverfassungsgerichts zum Lauschangriff. Obwohl es unmittelbar nur für die Strafprozessordnung gilt, hat es doch auch Auswirkungen auf das Bremische Polizeigesetz und die geplante Novellierung des bremischen Verfassungsschutzgesetzes.

Im Lande Bremen selbst hat der Datenschutz in den letzten Jahren ein Ziel erreicht. Er muss sich von wenigen Ausnahmen abgesehen nicht mehr in Erinnerung rufen, sondern die öffentlichen Stellen kommen mit ihren Problemen zu mir und lassen sich umfassend beraten oder entwickeln selbst gute Datenschutzkonzepte. So enthält dieser Bericht auch weitestgehend keine Mängellisten über Datenschutzverstöße, sondern kann über viele Erfolge berichten. Ebenso ist im privaten Sektor ein deutlicher Sinneswandel zu verspüren. „Privacy sells!“. Auch hier hat man verstanden, was dieser Slogan in knapper Form zum Ausdruck bringt.

1.1 Auditverordnung zum Bremischen Datenschutzgesetz

Die nach § 7 b Bremisches Datenschutzgesetz (BremDSG) vorgesehene Auditverordnung ist am 15. Oktober 2004 in Kraft getreten (Brem.GBl. 2004, S. 515). Bremen hat damit den Bund überholt, der seine Auditregelung noch nicht umgesetzt hat, und ist nach Schleswig-Holstein das zweite Bundesland mit einem Datenschutzaudit. In Bremen kann jetzt das Datenschutzaudit in der Praxis zum Einsatz kommen. Öffentliche Stellen Bremens können zur Verbesserung des Datenschutzes und der Datensicherheit ihre Verfahren einschließlich der dazugehörigen technischen Einrichtungen durch unabhängige Gutachter prüfen und bewerten lassen.

Ziel des Datenschutzaudits ist die Verbesserung des Datenschutzes und der Datensicherheit. Nach erfolgreicher Durchführung eines Datenschutzauditverfahrens durch einen externen Gutachter wird dem geprüften Verfahren ein datenschutzrechtliches Gütesiegel verliehen, mit dem die datenverarbeitende Stelle hinsichtlich ihrer Vertrauenswürdigkeit werben kann. Durch das Audit soll die Selbstverantwortung der Datenverarbeiter gefördert werden. Ein geprüftes Verfahren erhält durch die Auditierung Akzeptanz nach außen. Das Datenschutzgütesiegel ermöglicht es Bremer Stellen darüber hinaus, z. B. ihre Software-Produkte in anderen Ländern besser zu vermarkten, und schafft so auditierten Stellen einen Wettbewerbsvorteil. Wegen der rasanten technischen Weiterentwicklung wird das Datenschutzaudit-Gütesiegel auf zwei Jahre befristet erteilt. Für Verlängerungen besteht aber die Möglichkeit eines vereinfachten Verfahrens.

1.2 Einführung der elektronischen Arbeitszeiterfassung

Der Rechnungshof hat im Jahr 1992 die Einführung einer elektronischen Arbeitszeiterfassung in der bremischen Verwaltung gefordert. In der Folgezeit sind verschiedene Modelle erörtert und von mir datenschutzrechtlich begleitet worden. Daraus sind die „Grundsätze für die gleitende Arbeitszeit“ entstanden, die festlegen, dass ein Datenschutz- und ein Sicherheitskonzept sowie eine Verfahrensbeschreibung zu erstellen sind. Rechtliche Grundlage für die Arbeitszeiterfassung ist eine Dienstvereinbarung vom März 1999. Darin werden auch die zulässigen Kontrollen durch Vorgesetzte geregelt. Besonderes Augenmerk habe ich darauf gerichtet, dass keine heimlichen Kontrollen hinter dem Rücken der Beschäftigten stattfinden Über die Datenschutzaspekte habe ich auch im Rechtsausschuss berichtet. Ende des Jahres waren ca. 30 Dienststellen an das zentrale System angeschlossen.

1.3 eGovernment

Die staatlichen und kommunalen Stellen im Land Bremen bieten ihre Serviceleistungen zunehmend auf elektronischem Wege an, um damit unabhängig von Öffnungs- oder Wartezeiten, Parkplatzproblemen und anderen Hürden den Kontakt zu ihnen zu ermöglichen. Das Motto der elektronischen Verwaltung lautet: "Nicht die Bürger sollen laufen, sondern die Daten". Umfangreiche Online-Informationen über Verwaltungsdienstleistungen, Erreichbarkeit der Beschäftigten per E-Mail, Formular-Downloads und andere Internetanwendungen vereinfachen die Verfahrensabläufe und sollen die Kosten für die öffentliche Verwaltung senken. Dieser Prozess wird sich auch in den nächsten Jahren fortsetzen.

Die Bürger erwarten dabei von der Verwaltung kürzere Bearbeitungszeiten und niedrigere Kosten. Ob sich dabei die Hoffnungen auf weniger Bürokratie durch eGovernment verwirklichen lassen oder sich, wie einige befürchten, doch nur eine E-Bürokratie entwickelt, bleibt abzuwarten. Die Reformaktivitäten zielen dabei vornehmlich auf Massenverfahren wie im Bereich Melde- und Kfz-Wesen oder bei den elektronischen Steuererklärungen ab.

Untersuchungen haben ergeben, dass die Mehrheit der Bürger die Web-Angebote der öffentlichen Verwaltung in erster Linie zur reinen Informationsbeschaffung nutzen. Immerhin 47 % der regelmäßigen Internet-Nutzer nehmen Verwaltungsdienstleistungen über das Internet in Anspruch. Deutschland liegt im internationalen eGovernment-Ranking im hinteren Mittelfeld auf Platz 14. Rund 18 % der Web-User haben Bedenken, dass der Datenschutz beim eGovernment möglicherweise unzureichend sei.

Dies verdeutlicht einmal mehr, dass eine hohe Akzeptanz der Bürger nur dann erreicht werden kann, wenn Datenschutz und Datensicherheit gewährleistet sind. Voraussetzung dafür ist eine sichere und vertrauliche Kommunikation zwischen Bürgern und der Verwaltung, die einen angemessenen Schutz der personenbezogenen Daten gewährleistet. Ich habe gemeinsam mit den anderen Datenschutzbeauftragten des Bundes und der Länder Handlungsempfehlungen für ein "Datenschutzgerechtes eGovernment“ erarbeitet. Darin werden die spezifischen Anforderungen und Risiken, die mit dem eGovernment verbunden sind, ausführlich beschrieben. Einen großen Raum nehmen konkrete Empfehlungen und die Beschreibung von technischen und organisatorischen Schutzmaßnahmen ein. In einer Risikoanalyse sind die spezifischen Gegebenheiten zu betrachten und daraus technische und organisatorische Maßnahmen abzuleiten. IT-Verantwortliche können die aufgelisteten Handlungsempfehlungen als Checklisten nutzen, um Maßnahmen und Vorkehrungen für datenschutzgerechte und sichere eGovernment-Anwendungen festzulegen. Für die Bürger sind insbesondere die vorgestellten Instrumente des Selbst-Datenschutzes von großer Bedeutung.

Darüber hinaus habe ich mich im Berichtszeitraum intensiv um die Entwicklung der virtuellen Poststelle gekümmert. Dabei habe ich selbst an dem Pilotverfahren der bremischen Verwaltung teilgenommen, um so praktische Erfahrungen zu sammeln. Dadurch fällt es mir leichter, die notwendigen Schutzkonzepte zu entwickeln (Näheres vgl. Ziff. 3.1 dieses Berichts). In diesem

Zusammenhang verweise ich auf die Ausarbeitung „Die virtuelle Poststelle im datenschutzgerechten Einsatz“. Das Dokument kann in Kürze von meiner Homepage heruntergeladen werden.

1.4 Behördliche Datenschutzbeauftragte

Mit der Novellierung des Bremischen Datenschutzgesetzes (BremDSG) im Dezember 2002 wurde eine Norm aufgenommen, die die öffentlichen Stellen in Bremen und Bremerhaven zur Bestellung eines behördlichen Datenschutzbeauftragten verpflichtet (vgl. § 7 a BremDSG). Die Bestimmung regelt die Stellung des behördlichen Datenschutzbeauftragten innerhalb der öffentlichen Stelle, seine Aufgaben sowie Anforderungen an Eignung und Qualifikation. Die öffentlichen Stellen haben dem Landesbeauftragten für den Datenschutz die Bestellung und Beendigung eines behördlichen Datenschutzbeauftragten zu melden. Entsprechende Regelungen gibt es auch im Bundesdatenschutzgesetz und in Datenschutzgesetzen anderer Länder. Die Privatwirtschaft ist seit jeher verpflichtet, betriebliche Datenschutzbeauftragte zu bestellen.

Bedauerlicherweise hatte ich von einem Großteil der verpflichteten Stellen in 2003 keine Meldung über eine Bestellung gem. § 7 a Abs. 5 BremDSG erhalten. Entweder hatte man die Bestellung nicht vorgenommen oder mir nach einer Bestellung diese nicht gemeldet. Diese Stellen forderte ich auf, ihrer gesetzlichen Verpflichtung nachzukommen. In diesem Zusammenhang wies ich darauf hin, dass mehrere Stellen gemeinsam einen behördlichen Datenschutzbeauftragten bestellen können, nicht jede Stelle also einen eigenen Datenschutzbeauftragten bestellen muss, was insbesondere für kleinere Einrichtungen von Bedeutung sein dürfte.

Mittlerweile haben ca. 80 % aller Dienststellen der bremischen Verwaltung einen behördlichen Datenschutzbeauftragten gemeldet. In den restlichen Fällen sind häufig noch Rechtsfragen zu klären, die z. B. die Eignung und Qualifikation eines für das Amt des behördlichen Datenschutzbeauftragten vorgesehenen Mitarbeiters betreffen. Zur Qualifizierung biete ich Schulungen im Aus- und Fortbildungszentrum der bremischen Verwaltung an. Die bisherige Resonanz war sehr gut.

Aus dem Bereich des Magistrats der Stadt Bremerhaven habe ich bisher keine Meldung nach § 7 a Abs. 5 BremDSG erhalten. Ende 2004 sind mir vom Magistrat Überlegungen vorgestellt worden, grundsätzlich für jeweils ein Dezernat einen behördlichen Datenschutzbeauftragten zu bestellen. Aufgrund der Größe der Ämter und Einrichtungen in einem Dezernat oder besonderer für sie geltender Rechtsvorschriften ist geplant, für ein Amt allein oder dezernatsübergreifend einen behördlichen Datenschutzbeauftragten zu bestellen. Auch bei den Wirtschafts- und Eigenbetrieben stehen noch einige Meldungen über die Bestellung eines behördlichen Datenschutzbeauftragten aus.

1.5 Datenschutzrechtliche Beratung neuer Rechtsvorschriften im Land

Im Juli 2004 traten die Vorschriften des Bremischen Hafensicherheitsgesetzes in Kraft (Brem.GBl. 2004, S. 405). Mit den Änderungen soll den Anforderungen aus dem Konzept zur „Maritimen Sicherheit“ Rechnung getragen werden, ich berichtete hierzu ausführlich (vgl. 26. JB, Ziff. 12.2). Weiter habe ich Änderungen im Landesmediengesetz (vgl. Ziff. 2.3 dieses Berichts) und im Bremischen Wassergesetz beraten (Brem.GBl. 2004, S. 595), die die Erhebung von Daten zum Zwecke von Hochwasserschutzgebühren bei Grundstücksbesitzern betreffen. Zu erwähnen ist auch die Einfügung des § 46 a in das Bremische Abgeordnetengesetz (Brem.GBl. 2004, S. 597). Anlass war die beabsichtigte Nutzung der aus den USA zurückgeführten sog. Rosenholzdateien. Die Überprüfung von Abgeordneten auf Stasi-Kontakte ist ein Eingriff in deren informationelles Selbstbestimmungsrecht und kann daher nur auf Grund einer Einwilligung oder einer gesetzlichen Ermächtigung erfolgen. Ein mehrheitlicher Beschluss des Parlaments wäre hingegen keine ausreichende Grundlage für eine solche Datenabfrage. Es ist daher zu begrüßen, dass mit der Schaffung einer gesetzlichen Grundlage Rechtsklarheit geschaffen wurde. Schließlich habe ich den aus dem Hause des Senators für Bildung und Wissenschaft stammenden Arbeitsentwurf zur Novellierung des bremischen Schuldatenschutzgesetzes beraten, der sich nunmehr in der hausinternen Abstimmung befindet (vgl. Ziff. 10.3 dieses Berichts). Auch zu Novellierungsvorschlägen aus dem Innenressort, das Bremische Polizeigesetz und das bremische Verfassungsschutzgesetz betreffend, habe ich Stellungnahmen abgegeben (vgl. Ziff. 6.9 und Ziff. 6.10 dieses Berichts).

1.6 www.datenschutz4school ist gestartet

Mit Unterstützung aus dem Hause des Senators für Bildung und Wissenschaft habe ich das Online-Lernprojekt „datenschutz4school“ entwickelt. Am 22. Dezember 2004 ging die Lerneinheit online. Sie wird im Rahmen des Computerunterrichtes an Schulen eingesetzt, ein pädagogisches Konzept für die Lehrerinnen und Lehrer ist hinterlegt.

Zielgruppe sind Schülerinnen und Schüler zwischen zwölf und 15 Jahren. Schüler gehen schon in jungen Jahren ins Internet und haben häufig keine Vorstellung davon, wie viele Spuren sie dort hinterlassen. Um ein Bewusstsein dafür zu schaffen, habe ich an Lebenslagen der Jugendlichen orientiert eine Reihe von Informationen zusammengestellt - im Internet natürlich, wo sonst. Die Adresse lautet: „www.datenschutz4school.de“. Mit dem Angebot sollen Jugendliche für den Datenschutz sensibilisiert werden. Sie sollen lernen, wie sie sich selbst um ihre Belange beim Datenschutz kümmern können und welche Rechte sie haben.

Die Lerneinheit „datenschutz4school“ gliedert sich in vier Kapitel. Jedes Kapitel wird durch ein Tier der Bremer Stadtmusikanten animiert. Die Kapitel beinhalten am Ende ein oder zwei im Quizformat aufgemachte Tests zur Überprüfung des Erlernten. Mit richtigen Antworten kann man Bonus-Punkte sammeln, die in einem anschließenden Spiel eingesetzt werden können. Spielziel ist die richtige Anordnung der Bremer Stadtmusikanten in einer Slotmachine. Die besten Ergebnisse können in einer Top-10-Highscoreliste unter Angabe der Schule eingetragen werden. Die ständig wechselnden Eintragungen bereits in den ersten Wochen seit dem Start in der Liste zeigen, dass die Seite stark frequentiert wird.

1.7 Erweiterte Datenbasis bei der GEZ

Im Berichtsjahr habe ich zusammen mit anderen Datenschutzbeauftragten der Länder eine Datenschutzprüfung bei der GEZ durchgeführt. Da die GEZ gerade dabei ist, ein neues DV-Verfahren einzuführen, konnte dieses mit einbezogen werden. Der Prüfbericht befindet sich seit Anfang 2005 in der Abstimmung, die wesentlichen Ergebnisse können daher erst im nächsten Jahresbericht dargestellt werden.

Im Berichtsjahr wurden von den Ministerpräsidenten ohne vorhergehende Beteiligung der Datenschutzbeauftragten - wie es z. B. im Bremischen Datenschutzgesetz (BremDSG) vorgesehen ist - Änderungen im Rundfunkgebührenstaatsvertrag beschlossen. Unter anderem darf sich danach die GEZ bei kommerziellen Adresshändlern Daten beschaffen. Damit wird zusätzlich zu dem aus Sicht des Datenschutzes problematischen Zugriff auf Daten des Melderegisters im Zusammenhang mit der Gebührenerhebung der Rundfunkanstalten ein weiteres Tor für eine unverhältnismäßige Datensammlung geöffnet. Die Konferenz der Datenschutzbeauftragten hat stets die Praxis der GEZ kritisiert, jährlich mehrere Millionen Adressen ohne Kenntnis der Betroffenen beim kommerziellen Adresshandel zu beschaffen (Näheres vgl. Ziff. 2.2 dieses Berichts). Einen nicht unwesentlichen Anteil machen bei mir jedes Jahr Bürgerbeschwerden über oft unsinnige Schreiben aus Mailingverfahren der GEZ aus, bei denen offensichtlich Daten aus dem Adresshandel verwendet wurden. Es wäre daher an der Zeit, stattdessen die von den Datenschutzbeauftragten seit langem geforderte grundsätzliche datenschutzfreundliche Neuorientierung bei der Finanzierung des öffentlich-rechtlichen Rundfunks in Angriff zu nehmen (vgl. Entschließung der Konferenz „Neuordnung in der Rundfunkfinanzierung“, 26. JB, Ziff. 18.9).

1.8 Gravierende Datenschutzmängel beim Arbeitslosengeld II (ALG II)

Immer neue Probleme und Pannen tauchen mit dem Computerprogramm „A2LL“ auf, das die Grundlage für die Gewährung und Abrechnung des Arbeitslosengeldes II (ALG II) bildet. Verzögerte erst ein Stellenfehler bei den Kontonummern der Leistungsempfänger in Teilbereichen die Auszahlung des Arbeitslosengeldes, konnten danach Barschecks mit der Post nicht zugestellt werden, weil das Programm nach einer bestimmten Anzahl von Zeichen die Straßennamen abkürzte. In diese Reihe gliedern sich auch die zahlreichen, zum Teil erheblichen technischen und tatsächlichen Datenschutzmängel ein, die bei der praktischen Umsetzung der Zusammenführung von Arbeitslosen- und Sozialhilfe aufgetreten sind. Sie betreffen sowohl die Datenerhebung als auch die Leistungsberechnung. Besonders gravierend sind die unbeschränkten bundesweiten Zugriffsmöglichkeiten der sachbearbeitenden Kräfte auf alle von ALG II erfassten Daten. Wie sensibel diese Daten sein können, braucht an dieser Stelle nicht näher hervorgehoben werden. Da keine Protokollierung der Datenzugriffe erfolgt, können Missbräuche nicht erkannt und daher auch nicht aufgeklärt und abgestellt werden.

Auch in Bremen lief die Einführung des Computerprogramms „A2LL“ nicht reibungslos, in Bremerhaven kam es darüber hinaus im Vorfeld der Datenerhebung zu datenschutzrechtlichen Unzulänglichkeiten (vgl. Ziff. 9. dieses Berichts).

1.9 Steuerzahler in der informationellen Zwangsjacke

Es scheint, als handele der Gesetzgeber nach dem Motto: „Wozu brauchen wir noch die Angaben des Steuerbürgers, holen wir uns doch die Angaben lieber gleich direkt bei den Banken und anderen Stellen“. Will man sich ein Bild von der Entwicklung der steuerrechtlichen Überwachungsinstrumente machen, muss man die verschiedenen gesetzlichen Initiativen in diesem Bereich im Zusammenhang sehen. Zu nennen sind z. B. die elektronische Übertragung des Jahreseinkommens durch den Arbeitgeber an die Steuerverwaltung, die Mitteilungen der Kreditwirtschaft über die Inanspruchnahme von Freistellungsaufträgen, die Regelungen im Gesetz zur Förderung der Steuerehrlichkeit und die Einführung der Steueridentifikationsnummer wie auch verschiedene sog. Kontrollmitteilungen.

Die Steueridentifikationsnummer wird jedem Neugeborenen bereits in die Wiege gelegt. Auf die mit dieser Entwicklung verbundenen Gefahren, insbesondere eines verfassungsrechtlich unzulässigen Personenkennzeichens, hat die Konferenz der Datenschutzbeauftragten in der Entschließung „Personennummern“ hingewiesen (vgl. Ziff. 15.1 dieses Berichts).

Aber auch das Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003 (BGBl. I 2003, S. 2928) steht nach dem Auslaufen der Amnestieregelung im Blickpunkt des öffentlichen Interesses. Die Regelungen in § 93 Abs. 7 und 8 sowie in § 93 b der Abgabenordnung (AO) räumen Behörden und Gerichten weitreichende Möglichkeiten ein, sich durch automatisierten Datenabruf einen Überblick über alle Kontostammdaten einer Person zu verschaffen; sie sollen am 1. April 2005 in Kraft treten. Damit wird einer Vielzahl weiterer öffentlicher Stellen der Zugriff auf einen Datenpool ermöglicht, der nach § 24 c des Kreditwesengesetzes (KWG) im Rahmen der Terrorismusbekämpfung bisher nur den Finanzaufsichtsbehörden und den Strafverfolgungsbehörden zur Verfügung stand. Viele finden es bedenklich, wenn der Staat das gleiche System, das er zur Bekämpfung des Terrorismus eingeführt hat, für die umfassende Kontrollen aller redlichen Steuerbürger einsetzen will. Dabei gibt es bisher keine Untersuchungen darüber, ob Steuerhinterziehung, der das Gesetz entgegen treten will, wirklich ein allgemeines Phänomen ist.

Bei den in Rede stehenden Kontoinformationen handelt es sich neben den Depot- oder Kontonummern insbesondere um die Namen und Geburtsdaten der Inhaber und der Verfügungsberechtigten sowie um die Namen und Anschriften der sonst wirtschaftlich Berechtigten. Die Kontostände sind nicht Bestandteil der Abrufinformation, sie können aber unter Umständen im Rahmen weiterer Überprüfungen erhoben werden.

Damit stellt der Gesetzgeber den Finanzbehörden ein totales Überwachungsinstrument zur Verfügung. Alle Konten befinden sich im Zugriff der Finanzbehörden, das Taschengeldkonto eines Kindes ebenso wie die Konten vieler Bürgerinnen und Bürger, die nicht steuerpflichtig sind. Das Gesetz schießt damit über das Ziel weit hinaus.

Zusammengefasst wird mit der Einführung dieses umfassenden Kontrollsystems unterstellt, eine Vielzahl der Steuerpflichtigen nehme es mit der Steuerehrlichkeit nicht ernst. Ich bin mir hingegen sicher, dass die ganz überwiegende Mehrzahl der Betroffenen allein auf Grund ihres

Beschäftigungsverhältnisses oder ihrer wirtschaftlichen Situation keine Möglichkeiten hat, Steuern zu hinterziehen.

Die vorgesehenen Regelungen begegnen in mehrfacher Hinsicht datenschutzrechtlichen Bedenken. Der Abruf kann hinter dem Rücken der Betroffenen erfolgen, denn es ist nicht sichergestellt, dass die Betroffenen von einem automatisierten Abruf ihrer Daten überhaupt etwas erfahren. Nach den bis dato bekannt gewordenen Vorstellungen des Bundesfinanzministeriums sollen die Betroffenen von einer automatisierten Anfrage ihrer Daten nur dann etwas erfahren, wenn diese Abfrage zu klärungsbedürftigen Tatbeständen führt und die Betroffenen damit konfrontiert werden. Damit würde es von Zufälligkeiten abhängen, ob die Betroffenen vom Datenabruf erfahren oder nicht. Hier wird verkannt, dass jeder Datenabruf ein Eingriff in das informationelle Selbstbestimmungsrecht bedeutet. Eine solche Vorgehensweise widerspräche daher dem verfassungsrechtlichen Transparenzgebot und würde auch die Rechtsschutzgarantie des Art. 19 Abs. 4 Grundgesetz (GG) unterlaufen.

Die Finanzbehörden sollen darüber hinaus für andere Behörden - welche dies sind, wird im Gesetz nicht hinreichend genau bezeichnet - Kontoinformationen abfragen. Nach § 93 Abs. 8 AO sollen diese Behörden auf ein entsprechendes an die Finanzbehörden gerichtetes Ersuchen im Wege eines automatisierten Abrufs Kontodaten erhalten können, wenn sie ein Gesetz anwenden, das „an Begriffe des Einkommensteuergesetzes anknüpft“, und eigene Ermittlungen ihrer Versicherung nach nicht zum Ziel geführt haben oder aber keinen Erfolg versprechen.

Die Regelungen in diesem Teil des Gesetzes sind nicht normenklar. Außerdem hat es die Finanzbehörden nicht zu interessieren, mit welchen anderen Behörden jemand mit welchen Fragen im Kontakt steht. Die funktionale Trennung bei der Informationsverarbeitung wird durch diese Regelung nicht eingehalten. Angesichts der Vielzahl von Begriffen im Einkommensteuergesetz ist ein „Anknüpfen" an solche Begriffe sehr weitreichend und nur schwer eingrenzbar. Damit bleibt für den Bürger letztlich unklar, welche Behörden unter welchen Voraussetzungen berechtigt sind, solche Ersuchen an die Finanzbehörden zu richten.

Die Datenschutzbeauftragten des Bundes und der Länder sind sich einig, dass diese Regelungen so keinen Bestand haben dürfen. Dies haben sie in ihrer Entschließung „Staatliche Kontrolle muss auf den Prüfstand" zum Ausdruck gebracht (vgl. Ziff. 15.10 dieses Berichts).

1.10 JobCard

Das Bundeswirtschaftsministerium plant die Einführung einer zentralen Speicherstelle (ZSS), in der Arbeits- und Einkommensdaten der abhängig beschäftigten Bevölkerung Deutschlands gespeichert werden sollen. Dabei handelt es sich nicht um eine Chipkartenanwendung, auf der sämtliche Daten gespeichert werden, sondern um ein DV-Verfahren unter Einsatz einer Chipkarte. Mit der Entwicklung dieser zentralen Datenbank soll eine Entlastung der Wirtschaft einhergehen, die zur Zeit entsprechende Bescheinigungen ausstellen muss, wenn staatliche oder kommunale Leistungen wie Arbeitslosengeld, Wohngeld, Kindergeld etc. beantragt werden. Wie Arbeitgeber mit nur wenigen Beschäftigten dem gerecht werden können, bleibt abzuwarten.

So sieht das Verfahren zum Beispiel vor, dass bei einer Kündigung des Arbeitsverhältnisses dem Arbeitnehmer keine Arbeitsbescheinigung in Papierform mehr ausgestellt wird, sondern die Daten in elektronischer Form an die ZSS übermittelt werden. Der Arbeitgeber wird so davon entbunden, eine Arbeitsbescheinigung auszudrucken und zu archivieren. Die Bundesagentur für Arbeit soll dann mit den elektronisch zur Verfügung gestellten Daten ohne Nachfrage bei den Betroffenen den Leistungsanspruch berechnen und einen Bewilligungsbescheid erstellen. Da die Daten der Arbeitsbescheinigungen über sieben Jahre gespeichert werden sollen und auch eine Widerspruchsfrist einzurechnen ist, muss davon ausgegangen werden, dass in der ZSS mehrere Millionen Datensätze gespeichert sein werden. Vorgesehen ist dabei, dass der Arbeitgeber grundsätzlich das Entgelt und die Beschäftigungsdauer eines jeden Arbeitnehmers zur ZSS meldet, ungeachtet dessen, ob diese Daten tatsächlich einmal für eine Leistungsberechnung benötigt werden oder nicht. Damit wäre eine Gesamtsicht über das Berufsleben der gespeicherten Personen möglich. Ist dies schon allein aus datenschutzrechtlicher Sicht bedenklich, tritt hinzu, dass es Überlegungen gibt, die Rentenversicherungsnummer zur Generierung einer Identifikationsnummer zu nutzen. Das vollständige Szenario ist damit aber bei weitem noch nicht entwickelt. Denn ist erst einmal die Infrastruktur mit dem JobCard-Verfahren geschaffen, gehen die weiteren Überlegungen dahin, die abrufberechtigten Stellen um jene Behörden und Institutionen zu erweitern, die für die Leistungsgewährung zuständig sind. Derzeit laufen bereits Modellversuche zur technischen Machbarkeit, die bis zum 30. Juni 2005 abgeschlossen sein sollen. Anschließend soll mit der bundesweiten Realisierung begonnen werden; geplant ist, das Verfahren zum 1. Januar 2007 für alle Arbeitnehmer verpflichtend einzuführen.

Ich habe prinzipielle Bedenken gegen alle DV-Verfahren, die mit einem totalen Ansatz zentral in einer Datei und nicht in verteilten Systemen die Daten verwalten. Nur wenn neben rechtlichen Sicherungen auch die technische Umsetzung Gefährdungen für das Recht auf informationelle Selbstbestimmung ausschließt, kann eine zentrale Lösung gegebenenfalls hingenommen werden. Die Konferenz der Datenschutzbeauftragten hat eine gemeinsame Arbeitsgruppe gebildet, an der auch ich mich beteilige, und diese beauftragt, das Vorhaben zu begleiten. Die in der Arbeitsgruppe vertretenen Landesbeauftragten für den Datenschutz haben eine Revision des bisherigen Konzepts gefordert mit dem Ziel, die schon bisher vorgesehene Verschlüsselung der Daten in die Hände der betroffenen Beschäftigten zu geben. Damit soll vermieden werden, dass eine Zweckentfremdung oder ein

Missbrauch der bei der ZSS gespeicherten Daten stattfinden kann. Die Konferenz der Datenschutzbeauftragten vom 28. und 29. Oktober 2004 hat den Vorschlag der Arbeitsgruppe einer Ende-zu-Ende-Verschlüsselung mit einem in den Händen des Betroffenen liegenden Schlüssels aufgegriffen und das Bundeswirtschaftsministerium gebeten, die Realisierbarkeit dieses Konzepts durch einen neutralen Gutachter überprüfen zu lassen.

1.11 Droht der genetisch gläserne Mensch?

In dem Maße, wie die Kosten für genetische Tests sinken, steigt das Interesse vieler Stellen, das menschliche Erbgut zu untersuchen und die Ergebnisse der Analyse für verschiedene Zwecke zu verwerten. An vorderster Stelle sind Forschungslabors, Pharmaindustrie, Versicherungen und Arbeitgeber zu nennen. Zurzeit sind die hoch sensiblen Informationen, die in der DNS eines jeden Menschen enthalten sind, nicht ausreichend gegen Untersuchungen geschützt, die auch heimlich durchgeführt werden können. Hierauf hat die Konferenz der Datenschutzbeauftragten bereits vor Jahren hingewiesen und in einer Entschließung in 2001 gesetzliche Regelungen über die Durchführung von genetischen Untersuchungen gefordert (vgl. 24. JB, Ziff. 15.11).

Diesen Forderungen wurde leider bis heute nicht Rechnung getragen. Erst als eine Krankenkasse im Zusammenwirken mit der Medizinischen Hochschule Hannover bei 6.000 ihrer Versicherten einen Massengentest durchführen wollte, wurden in Reaktionen darauf erneut Stimmen laut, die rasche gesetzliche Regelungen verlangten. Das Gesundheitsministerium ist unter dem Arbeitstitel „Gesetzentwurf zur Gendiagnostik“ dabei, entsprechende Regelungen vorzubereiten. Leider wurde diese unterstützenswerte Arbeit in der Öffentlichkeit bisher generell nicht genügend gewürdigt und kritisch begleitet; nur eine nicht einmal den Kernbereich tangierende Facette wurde in den Medien und an den Stammtischen diskutiert: Der (heimliche) Vaterschaftstest. Allen Zweiflern in der Frage hat dann der BGH in seinem Urteil vom 12. Januar 2005 (AZ. XII ZR 60 und 227/03) den rechten Weg gewiesen und entschieden, dass die Untersuchung des genetischen Materials eines anderen Menschen ohne dessen ausdrückliche Zustimmung gegen das Grundrecht auf informationelle Selbstbestimmung verstoße und rechtswidrig sei. Dieses Grundrecht des Kindes brauche auch nicht hinter dem Interesse des als Vater geltenden Mannes zurückzustehen, der sich Gewissheit über seine biologische Vaterschaft verschaffen möchte.

Die Abwägungen, die im Zentrum solcher diesen Bereich regelnden Normen stehen, sind nicht nur verfassungs- und datenschutzrechtlicher, sondern auch ethischer und medizinischer Natur. Es geht im Wesentlichen darum, den Betroffenen vor ungewollten und unzulässigen Ausforschungen seiner Erbinformationen zu schützen und sein Selbstbestimmungsrecht auch in diesem Bereich zu sichern. Dies beinhaltet auch, nicht zu wissen, ggf. welche problematischen Genkonstellationen man selbst hat. Nur so kann sichergestellt werden, dass erbliche Veranlagungen und kritische genetische Konstellationen nicht missbraucht werden oder zu einer Diskriminierung führen.

Gentests bei Neugeborenen und Gen-Datenbanken: Alarmiert durch die Meldungen der Presse, die EU plane Gentests für alle Neugeborenen, sah ich mich veranlasst, den Hintergründen nachzugehen. Ein solches Screening würde die reihenweise Untersuchung einer bestimmten Gruppe auf eine oder mehrere definierte Krankheiten beinhalten. Das Interesse an genetischen Untersuchungen auch bei Erwachsenen wächst. Auf die mit diesen Tendenzen verbundenen Datenschutzprobleme gehe ich im Bericht näher ein (vgl. Ziff. 8.3 dieses Berichts). Besondere Aufmerksamkeit verdient aus datenschutzrechtlicher Sicht das Vorhaben, genetische Daten zu Forschungszwecken in Datenbanken einzuspeisen.

Zusammenfassend lässt sich sagen: Das Interesse an Erbgutinformationen muss gesteuert werden, sonst droht der genetisch gläserne Mensch!

Genanalyse im Strafverfahren: Auf die Idee muss man erst einmal kommen: Den Mord an dem Prominenten Moshammer zum Anlass für eine Debatte zur Erweiterung der DNA-Analyse zu nehmen. Ja, hat man den vermeintlichen Täter denn nicht gefasst? Und hatte man ihn nicht binnen eines Tages identifiziert? Gab es Probleme mit den DNA-Analysedaten? Der Fall ist für diese Debatte völlig ungeeignet, verdeutlicht er doch vielmehr, dass die vom Gesetzgeber zur Verfügung gestellten Instrumente in der Strafprozessordnung ausreichen, um einen schnellen Fahndungserfolg sicherzustellen. Gleichwohl, der Fall Moshammer war Kumulationspunkt für eine unterschwellig seit Jahren insbesondere von Innenpolitikern auch in unserem Bundesland geführte Debatte zur Absenkung der Eingriffsvoraussetzungen und der verfahrenssichernden Maßnahmen für die personenbezogene Speicherung von DNA-Analyseergebnissen in einer Datei beim BKA.

Die Konferenz der Datenschutzbeauftragten hat sich in der Vergangenheit schon mehrfach mit Entschließungen zum Datenschutz bei der DNA-Analyse im Strafverfahren an die Öffentlichkeit gewandt und, als habe sie es kommen gesehen, bereits im Juli 2003 (vgl. 26. JB, Ziff. 18.10) mit der Entschließung „Bei der Erweiterung der DNA-Analyse Augenmaß bewahren“ die Antworten auf die jetzt entbrannte Diskussion formuliert.

Die Abschaffung des Richtervorbehalts würde die Bedeutung und Tragweite des von der Verfassung verbürgten Rechts auf informationelle Selbstbestimmung verkennen. Nur durch den Richtervorbehalt und der damit vorgeschalteten Überprüfungsentscheidung der Ermittlungsbehörden kann der Schwere des Eingriffs hinreichend Rechnung getragen werden. Die besondere Qualität des Grundrechtseingriffs schließt außerdem eine routinemäßige und undifferenzierte Anwendung des besonderen Ermittlungswerkzeuges DNA-Analyse bei Straftaten geringer Schwere aus.

Die Kritiker sollten die durch verfassungs- und obergerichtliche Entscheidungen getroffenen Festlegungen zur richterlichen Prüfpflicht nicht weiter in Frage stellen. Vielmehr sollten einige Bundesländer erst einmal die retrograde Erfassung aller nach den jetzigen Regelungen zulässigen Altfälle abschließen. Weiterhin erscheint statt einer Verbreiterung der Datenbasis wichtig, dass wenigstens europaweit ein einheitliches Testverfahren zugrunde gelegt wird, um die Vergleichbarkeit grenzüberschreitend sicherzustellen. Lediglich bei der Untersuchung anonymer Spuren und für die Durchführung von DNA-Massengentests besteht ein gesetzgeberischer Handlungsbedarf. Letzteres sage ich nicht zuletzt wegen der Erfahrungen, die ich beim in Bremerhaven durchgeführten DNA-Massentestverfahren an rund 2.200 Männern sammeln konnte (vgl. Ziff. 6.3 dieses Berichts).

1.12 Kein Lauschangriff im Kernbereich privater Lebensgestaltung

Am 3. März 2004 hat das Bundesverfassungsgericht (BVerfG) sein Urteil zum so genannten großen Lauschangriff gesprochen und die gesetzlichen Regelungen zur Wohnraumüberwachung in großen Teilen für verfassungswidrig erklärt (BVerfGE 1BvR 2378/98). Kritiker des Urteils beklagen, dass durch das Urteil das Instrument der akustischen Wohnraumüberwachung wertlos werde. Für mich hingegen stellt sich die Frage, ob nach dem Urteil des BVerfG der hohe Aufwand der Verfassungsänderung seinerzeit gerechtfertigt war.

Kernaussage in dem Urteil des BVerfG ist, dass die Anforderungen an die Rechtmäßigkeit der Wohnraumüberwachung umso strenger sein müssen, je größer das Risiko ist, dass mit ihnen Gespräche höchstpersönlichen Inhalts erfasst werden können. Führe die Überwachung unerwartet zur Erhebung von absolut geschützten Informationen, müssten die Überwachung abgebrochen und erhobene Aufzeichnungen gelöscht werden. Jegliche Verwendung solcher im Rahmen der Strafverfolgung erhobener geschützter Daten sei ausgeschlossen. Das Risiko, solche Daten zu erfassen, bestehe typischerweise beim Abhören von Gesprächen mit engsten Familienangehörigen, sonstigen engsten Vertrauten und Personen, zu denen ein besonderes Vertrauensverhältnis bestehe, wie z. B. bei Pastoren, Ärzten oder Strafverteidigern.

Die Datenschutzbeauftragten haben sich mit den Auswirkungen der Entscheidung zur akustischen Wohnraumüberwachung auseinandergesetzt und darauf aufmerksam gemacht, dass die Prinzipien der Entscheidung auch auf die Rechtslage in der Polizei und in den Nachrichtendiensten übertragen werden müssen (Entschließung vom 28./29. Oktober 2004, vgl. Ziff. 15.7 dieses Berichts). In diesem Zusammenhang bekräftigten die Datenschutzbeauftragten ihre Forderung, alle Formen der verdeckten Datenerhebung des Verfassungsschutzes, der Polizei sowie von Strafverfolgungsbehörden und anderen Sicherheitsbehörden an die Anforderungen der verfassungsgerichtlichen Entscheidung auszurichten und dazu zügig die gesetzlichen Änderungsverfahren einzuleiten.

Zur Novellierung der akustischen Wohnraumüberwachung hat die Bundesregierung den zweiten Entwurf einer Änderung der Bestimmungen der Strafprozessordnung vorgelegt. Nachdem der erste Entwurf insbesondere wegen der Einbeziehung der Berufsgeheimnisträger, wie beispielsweise Ärzte, Rechtsanwälte, Seelsorger und Journalisten, heftigen Protest hervorgerufen hat, werden diese Berufsgruppen als Instrument der akustischen Wohnraumüberwachung in der jetzigen Änderung nur dann mit erfasst, wenn sie als Teilnehmer des kriminellen Geschehens ebenfalls in Verdacht stehen. Zu den übrigen aus dem Urteil resultierenden Änderungen anderer Rechtsvorschriften stehen allerdings Gesetzgebungsvorhaben noch aus. Das gilt auch für die entsprechende Regelung im Bremischen Polizeigesetz. Hierauf habe ich den Senator für Inneres und Sport hingewiesen und ihm mitgeteilt, dass ich erwarte, dass von der Anwendung dieser Vorschrift abgesehen werde, bis eine verfassungskonforme Rechtslage hergestellt ist. Ein Vertreter des Senators für Inneres und Sport hat im Rechtsausschuss hierzu erklärt, man werde die Verfassungsrechtsprechung respektieren, man wolle aber zunächst die Gesetzgebung im Bund abwarten, bevor man die Rechtslage im Land Bremen anpasse.

1.13 Ausweise mit biometrischen Merkmalen

Welche Probleme mit der Einführung von Ausweisdokumenten mit integriertem Chip auf den biometrischen Merkmalen verbunden sind, habe ich bereits im letzten Jahr dargelegt (vgl. 26. JB, Ziff. 1.19). Nachrichten wie "Ausweise mit digitalen Merkmalen kosten über 600 Millionen Euro im Jahr" oder den Berechnungen des Büros für Technikfolgenabschätzung des Bundestages, das bis zu 300 Euro pro Pass annimmt, haben Bundesinnenminister Schily nicht davon abbringen können, die ersten Pässe dieser Art bereits im Herbst 2005 einführen zu wollen. Dabei sollen die Betriebskosten für Hard- und Software in den Meldestellen ein bestimmender Faktor sein, der die Kosten in die Höhe treibt.

Das Europäische Parlament hat Anfang Dezember 2004 in seiner Stellungnahme zur geplanten EU-Pass-Verordnung deutliche Verbesserungen zur Sicherung des Persönlichkeitsrechts gefordert. Mit der Pass-Verordnung sollen neben einheitlichen Sichtmerkmalen auch biometrische Merkmale in die Pässe und andere Reisedokumente der EU-Bürger eingeführt werden. Das Parlament lehnte die Speicherung der Passdaten aller EU-Bürger in einer zentralen Datei ab. Eine derartige Datenbank würde unverhältnismäßig sein und das Risiko des Missbrauchs und der Zweckentfremdung der sensiblen Daten erhöhen. Ebenfalls wurde durch das Europäische Parlament eine verpflichtende Aufnahme eines zweiten biometrischen Merkmals neben der Gesichtserkennung in die Ausweispapiere abgelehnt. Schließlich hat das EU-Parlament gefordert, die Behörden und sonstigen Stellen, die Zugang zu den in den Ausweispapieren auf einem integrierten Chip gespeicherten Daten haben sollen, in ein Register aufzunehmen, damit die notwendige Transparenz erreicht und Missbrauch weitestgehend vermieden wird. Damit werden viele Forderungen der Datenschutzbeauftragten aufgegriffen. Der Bundesbeauftragte für den Datenschutz hat in 2004 in einem Schreiben an den Vorsitzenden des EU-Rates auf Berichte aufmerksam gemacht, in denen darauf hingewiesen wird, dass bei Tests der biometrischen Verfahren diese die angestrebte Sicherheit nicht garantiert hätten. Die Zahl der Fälle, in denen das System Berechtigte zu Unrecht zurückgewiesen habe, sei ausgesprochen hoch gewesen.

1.14 Gläserner Kunde – Befürchtung oder Realität

Nicht nur im öffentlichen Sektor, sondern auch in der Privatwirtschaft geht der Trend zu immer umfangreicheren Datensammlungen und Datenverbundsystemen. Hierzu zählen Data-Mining-Systeme (zur Kritik an den Data-Mining-Systemen im Internet vgl. 23. JB, Ziff. 1.2 und CD „25 Jahre Datenschutz in Bremen“, Ziff. 4.1.3) ebenso wie das immer dichter werdende Netz verschiedener Warndateien. Neben zahlreichen Kreditauskunftssystemen entwickelt jetzt die Wohnungswirtschaft eigene Warndateien oder integriert diese in vorhandene Auskunftssysteme (vgl. Ziff. 14.8.1 dieses Berichts), aber auch die Versicherungswirtschaft verfügt über zentrale Warn- und Hinweissysteme. Anzuerkennen ist das legitime Interesse der Wirtschaft, sich vor Betrügern, schwarzen Schafen und zahlungsunfähigen oder -unwilligen Kunden zu schützen. Die einzelnen Auskunftssysteme sind in der Regel datenschutzrechtlich nicht zu beanstanden, gleichwohl müssen bei der Ausgestaltung dieser Systeme auch die schutzwürdigen Belange der Betroffenen in hinreichendem Maße Berücksichtigung finden. Gefahren entstehen dort, wo verschiedene Systeme vernetzt werden oder durch die Recherche über verschiedene Bereiche den einzelnen Kunden in seinen vielfältigen wirtschaftlichen Beziehungen durchleuchten. Es darf nicht dazu kommen, dass zum Beispiel ein junger Mensch, der mit 18 Jahren seine Handy-Rechnung nicht bezahlen konnte, anschließend kein Konto mehr eröffnen kann, keine Wohnung findet oder keine Versicherung mehr abschließen kann.

Auch die rasant zunehmende Einführung der RFID-Chip-Technologie gibt Anlass zur Besorgnis. Warenhersteller und Handel setzen zunehmend weltweit Radio-frequenz-gestützte Mikrochips (RFID-tags) zur Kennzeichnung von Warenbeständen wie auch zur Preisauszeichnung ein (Näheres vgl. 26. JB, Ziff. 1.25 „Mikrochips zum Aufbügeln“). Diese funkenden Mikrochips werden voraussichtlich in Kürze zu unserer täglichen Umgebung gehören. Ihre möglichen Auswirkungen auf die Privatsphäre sind weitreichend. Die Gefahr besteht, dass sie ein umfassendes Konsum-, Nutzungs-, Verhaltens- und Bewegungsprofil ermöglichen. Ich habe es daher für nötig gehalten, mich im Berichtsjahr umfassend über die technische Funktionsweise und die Gestaltungsmöglichkeiten zu informieren. Die wesentlichen Ergebnisse sind im Arbeitskreis „Technik“ der Datenschutzbeauftragten des Bundes und der Länder zusammengetragen worden, ich werde sie in Kürze auf meiner Homepage veröffentlichen.

1.15 Zur Entwicklung in der Telekommunikation

Der Bundesbeauftragte für den Datenschutz (BfD) berichtet, dass die Zahl der Telefonüberwachungen wiederum weiter deutlich angestiegen ist. So haben die Telekommunikationsunternehmen der Regulierungsbehörde für Telekommunikation und Post für das Jahr 2002 21.874 Anordnungen gemeldet. Die anschließende Zahl für das Jahr 2003 beträgt 24.441 Anordnungen (vgl. Graphik Ziff. 16.4 dieses Berichts). Der BfD berichtet, dass die Zahl der Anordnungen von Jahr zu Jahr steige und sich seit 1995 fast verfünffacht habe. Eine nachvollziehbare, befriedigende Erklärung hierfür gebe es nach wie vor nicht. Auch der Präsident des Bundesverfassungsgerichts äußerte sich im April 2004 zu dieser Entwicklung kritisch. Vor dem Hintergrund der internationalen Terrorgefahr warne er "dringend davor, das durchaus legitime Sicherheitsbedürfnis der Bevölkerung zu nutzen, um Freiheitsrechte gewissermaßen schon einmal vorsorglich und über das Maß der Verhältnismäßigkeit hinaus einzuschränken". Die Zahl der Telefonüberwachungen in Deutschland sei hoch und das Grundrecht des Fernmeldegeheimnisses werde „bereits in erheblichem Maße eingeschränkt".

Aber auch mit der Forderung nach einer im Bremischen Polizeigesetz geregelten präventiven Telefonüberwachung musste ich mich auseinandersetzen. Bislang ist das Abhören nur für Zwecke der Strafverfolgung zulässig, und zwar nur unter der Voraussetzung, dass eine Straftat von besonderem Gewicht vorliegt, besondere Tatsachen einen Verdacht begründen und ein Richter die Maßnahme angeordnet hat. Im Innenressort gibt es jedoch Überlegungen, Abhörmaßnahmen künftig auch für präventive Zwecke zuzulassen.

Zu bedenken ist, dass es im präventiven Bereich noch keine Beschuldigten gibt. Auch gibt es keine Gewissheit, dass bestimmte Straftaten tatsächlich begangen werden, wenn die Polizei sie nicht verhindert. In diesem unsicheren Raum würde durch eine solche Regelung die Überwachung der Bürger zulässig. Die präventive Telekommunikationsüberwachung als rein polizeiliches Mittel zur Gefahrenabwehr einzuführen, kann hinsichtlich der Anwendungsfälle problematisch sein. Gleichwohl gibt es in einigen Ländern bereits eine solche Regelung. Gegen die niedersächsische Regelung wurde eine Verfassungsbeschwerde beim Bundesverfassungsgericht erhoben. Die Konferenz der Datenschutzbeauftragten, die diesem Instrument kritisch gegenüber eingestellt ist, hat daher den Landesgesetzgebern empfohlen, vor der Schaffung neuer Bestimmungen in den Polizeigesetzen der Länder die voraussichtlich richtungsweisende Entscheidung des Bundesverfassungsgerichts abzuwarten.

Eine umfassende Vorratsspeicherung von Telekommunikationsdaten, wie sie im EU-Ministerrat beraten wird (vgl. Rats-Dok. 8958/04), wird von den Datenschutzbeauftragten des Bundes und der Länder kategorisch abgelehnt. Die Speicherung und Auswertung von ausgesuchten Internetadressen verrät etwas über die Interessen, Vorlieben und politischen Präferenzen der Nutzer. Damit verbunden wäre zugleich eine Verletzung der Grundrechte auf freie Meinungsäußerung und auf ungehinderte Unterrichtung aus allgemein zugänglichen Quellen. Das novellierte TKG enthält denn auch zum Glück eine solche Regelung nicht. Der Deutsche Bundestag hat seine mit diesen Regelungen zum Ausdruck kommende Ablehnung Anfang 2005 noch einmal bekräftigt (BT-Drs. 15/4597).

Leider enthält das im Berichtsjahr novellierte TKG (BGBl. I S. 1190) auch einige datenschutzrechtliche Verschlechterungen. So ist die Möglichkeit des anonymen Telefonierens mittels Prepaid-Cards (Entschließung der Konferenz „Geplanter genetischer Identifikationszwang in der Telekommunikation“, vgl. 25. JB, Ziff. 15.5) nicht mehr möglich, weil man sich beim Kauf einer solchen Karte nunmehr ausweisen muss. Ebenso wurde die Inverssuche grundsätzlich zugelassen. Wer mit dieser nicht einverstanden ist, muss aktiv werden und widersprechen (Näheres vgl. Ziff. 2.1 dieses Berichts).

1.16 Bürgeranfragen

Auch im Jahr 2004 erhielt ich zahlreiche Eingaben per Post oder E-Mail sowie durch Anrufe von Bürgern, Unternehmen und Behörden, die mich um die Klärung ihrer datenschutzrechtlichen Probleme baten. Dabei betrafen die Anfragen die unterschiedlichsten Bereiche der Datenverarbeitung. Am häufigsten ging es um Fragen des Arbeitnehmerdatenschutzes, der Datenverarbeitung der Auskunfteien, der Übermittlung personenbezogener Daten ins Ausland, der Videoüberwachung und der Tätigkeit behördlicher bzw. betrieblicher Datenschutzbeauftragter.

Etwa zwei Drittel der telefonischen Anfragen betrafen die Datenverarbeitung im nicht öffentlichen Bereich. Um die Vielfalt der Anfragen, die ich telefonisch erledigen konnte, zu dokumentieren, habe ich auszugsweise einige dieser Themen aus 2004 in einer Tabelle zusammengestellt (vgl. Anlage Ziff. 16.4 dieses Berichts).

Immer wieder möchten Bürger ihre Anliegen auch persönlich vortragen. Dies können sie nicht nur in meiner Dienststelle in Bremerhaven, sondern donnerstags in der Zeit von 15.00 Uhr bis 18.00 Uhr auch in Bremen, wo ich eine Bürgersprechstunde anbiete.

1.17 Öffentlichkeitsarbeit und Presseresonanz

Im vergangenen Berichtszeitraum habe ich zu diversen datenschutzrechtlichen Themen Pressemitteilungen herausgegeben, um insbesondere die Bremer Bürgerinnen und Bürger auf neue Entwicklungen im Datenschutz aufmerksam zu machen. Die Pressemitteilungen sind jeweils aktuell auf meiner Homepage www.datenschutz.bremen.de unter „Pressemitteilungen“ abrufbar. Darüber hinaus bin ich Anfragen der Medien nachgekommen und habe mich im Rahmen von Interviews und Stellungnahmen zu datenschutzrechtlichen Fragestellungen geäußert. Ein Überblick über die in der Presse behandelten Datenschutzthemen ist im Anhang (vgl. Pressespiegel Ziff. 16.1 dieses Berichts) zu finden.

Auf meiner Homepage veröffentliche ich neben den Pressemitteilungen weitere aktuelle Informationen zum Datenschutz unter „Aktuelles“ und „Tipps für Bürger“, die eine gute Resonanz finden.

1.18 Fortbildungsbeiträge vom LfD

Auch im letzten Berichtsjahr haben die in meiner Dienststelle Beschäftigten eine Vielzahl von Seminaren und Schulungen durchgeführt. Einige interessante Veranstaltungen führe ich nachfolgend auf:

- Fortbildung für den Führungskräftepool beim Senator für Finanzen im Aus- und Fortbildungszentrum Bremen,
- Referat „Data Mining/Data Warehouse: Elektronische Profile oder Datenschutz“ auf dem Workshop „Wissen ist was wert, Wissen ist flüchtig“ der Vereinten Dienstleistungsgewerkschaft ver.di e. V. in Bremen,
- Referat zum Mammographie-Screening im „Multidisziplinären Kurs“ am Klinikum Bremen-Mitte,
- Seminar zum Arbeitnehmerdatenschutz bei der Arbeitnehmerkammer Bremen,
- Seminar „Datenschutz im Personalwesen“ beim Aus- und Fortbildungszentrum Bremen,
- Vorlesungen über juristische Grundlagen in Datenschutz und Datensicherheit an der Hochschule Bremerhaven,
- Vortrag in Garlstedt vor behördlichen Datenschutzbeauftragten der Bundeswehr (auf Anfrage des BfD),
- Seminar für behördliche Datenschutzbeauftragte beim Aus- und Fortbildungszentrum Bremen,
- Vortrag „WLAN aus Sicht des Datenschutzes“ beim Senator für Finanzen,
- Mehrere Seminare “Sicherheit im Internet“ bei der Wirtschafts- und Sozialakademie der Arbeitnehmerkammer Bremen,
- Vortrag „eGovernment bei den Sicherheitsbehörden“ als Kooperationsveranstaltung des Senators für Finanzen und der Firma SEL,
- Seminar „Einführung in das Datenschutzrecht“ beim Aus- und Fortbildungszentrum Bremen.

1.19 Zur Situation der Dienststelle

Rückblickend muss ich feststellen: Es ist schon erstaunlich, wie schnell man sich an Gutes gewöhnen kann. Zur Erinnerung: Noch vor fünf Jahren verfügte die Dienststelle nur über Einzelplatz-PCs. Im Jahre 2000 konnte ich erreichen, dass ein Hausnetz in Betrieb ging, und erst vor drei Jahren waren alle Arbeitsplätze mit einem Internetanschluss ausgestattet. In 2003 wurde dann im Hause ein Dokumentenmanagementsystem eingeführt, das bisher voll und ganz die Erwartungen an eine Effektivierung der Bürokommunikation und Archivierung erfüllt hat. Die Administration des Hausnetzes wird intern durchgeführt. Im Berichtsjahr mussten der E-Mail-Server ersetzt und die technischen Vorbereitungen zur Einführung der elektronischen Arbeitszeiterfassung getroffen werden, die über ein zentrales Verfahren in Bremen abgewickelt wird.

Eine besondere Herausforderung war die Fertigstellung des Projekts "datenschutz4school" und die Durchführung des Workshops der Datenschutzaufsichtsbehörden (vgl. Ziff. 14.10 dieses Berichts), der mit freundlicher Unterstützung des Präsidenten der Bremischen Bürgerschaft in seinem Hause stattfinden konnte. Hierfür wie auch für andere offensichtlich gern gegebene Hilfestellungen aus seinem Hause sei an dieser Stelle gedankt.

Es ist nicht immer leicht, die vielen neuen technischen Entwicklungen datenschutzrechtlich zu bewerten. Hinzu kommen viele andere Anforderungen an meine Dienststelle, vielleicht vermitteln die Punkte „Durchgeführte Fortbildungsveranstaltungen" (vgl. Ziff. 1.18 dieses Berichts) und „Telefonische Anfragen“ (vgl. Ziff. 1.16 und Ziff. 16.2 dieses Berichts) neben den inhaltlichen Darstellungen der einzelnen Punkte eine gewisse Vorstellung von der Bandbreite der Fragestellungen und dem Arbeitseinsatz, der von allen Beschäftigten meiner Dienststelle erbracht werden muss, um den vielfältigen Anforderungen gerecht zu werden. Die Beschäftigten haben daher mit Genugtuung die Anerkennung, die im Rahmen der Parlamentsdebatte über den Bericht und Antrag des Rechtsausschusses zum 25. Jahresbericht in der Bremischen Bürgerschaft ausgesprochen wurde, zur Kenntnis genommen.

1.20 Kooperationen

Das Bremische Datenschutzgesetz beschreibt in § 27 Abs. 4 BremDSG die Zusammenarbeit mit anderen Datenschutzkontrolleinrichtungen. Die Zusammenarbeit mit den Datenschutzbeauftragten des Bundes und der Länder wie auch mit den Datenschutzaufsichtsbehörden, zuständig für den nicht öffentlichen Bereich, ist unabdingbare Voraussetzung, um den tatsächlichen, vielfältigen Herausforderungen einigermaßen gerecht zu werden. Die Entscheidungsschwerpunkte liegen dabei in der Konferenz der Datenschutzbeauftragtenden und im Düsseldorfer Kreis, allerdings wäre eine Entscheidungsfindung ohne eine effektive Unterstützung aus den Arbeitskreisen nicht möglich. Wesentliche Ergebnisse der Zusammenarbeit in der Konferenz der Datenschutzbeauftragten spiegeln sich in den Entschließungen der Konferenz wieder, die jeweils im Anhang meines Berichts zu finden sind (vgl. Ziff. 15 dieses Berichts).

Nicht unerwähnt bleiben soll an dieser Stelle auch die gute Kooperation mit der landeseigenen "datenschutz nord GmbH", mit der ich einen regelmäßigen Gedankenaustausch pflege und mit der ich auch im vergangenen Jahr wieder gemeinsam einige Projekte durchgeführt habe. Ebenso hervorzuheben ist die gute Zusammenarbeit mit dem Erfa-Kreis der betrieblichen Beauftragten für den Datenschutz der Region, an dessen Sitzungen ich regelmäßig teilnehme. Umgekehrt haben Mitglieder des Erfa-Kreises mich bei Lehrveranstaltungen und beim Workshop der Datenschutzaufsichtsbehörden unterstützt und diese durch ihre praktischen Erfahrungen belebt.

2. Telekommunikation, Teledienste und Medien

2.1 Novellierung des Telekommunikationsgesetzes

Am 26. Juni 2004 trat das novellierteTelekommunikationsgesetz in Kraft.

Inverssuche: Trotz des Vorbringens datenschutzrechtlicher Bedenken ist im neuen Telekommunikationsgesetz (TKG) die sog. Inverssuche vorgesehen. Mit dieser Suche lassen sich bei Angabe der Rufnummer Name und Adresse des Teilnehmers ermitteln. Diese Auskunft ist nur erlaubt, wenn der Teilnehmer im Teilnehmerverzeichnis (Telefonbuch oder öffentliches elektronisches Kundenverzeichnis) eingetragen ist und nach einem Hinweis seines Anbieters auf seine Widerspruchsmöglichkeit nicht widersprochen hat. Damit der Kunde den Hinweis auch tatsächlich wahrnimmt und nicht ungelesen wegwirft, darf dieser nicht wie Werbung aufgemacht sein. Zudem muss ausdrücklich im Hinweisschreiben auf das Widerspruchsrecht hingewiesen werden. Ich habe einen Hinweis auf das Widerspruchsrecht auch auf meiner Homepage.

Keine Anonymität mehr bei Kauf von Prepaid-Karten: Die Anbieter von Telekommunikationsdienstleistungen müssen aus Gründen der öffentlichen Sicherheit Namen und Anschrift des Kunden, die Rufnummer, Datum des Vertragsbeginns und das Geburtsdatum erheben und speichern. Der Anbieter darf außerdem die Vorlage eines amtlichen Ausweises verlangen, wenn dies zur Überprüfung der Angaben erforderlich ist. Die Verpflichtung zur Angabe der o. g. Daten gilt auch für den Kauf von Prepaid-Karten. Diese die Anbieter verpflichtende neue gesetzliche Regelung ist bedauerlich, da Prepaid-Karten eine anonyme Telefonkommunikation gegenüber einem Provider gewährleisten sollten.

Vorratsdatenspeicherung erfolgreich verhindert: Es war geplant, Daten über die Nutzungen von Telekommunikations- und Internetdiensten mindestens sechs Monate zu speichern. Diese geplante Vorratsdatenspeicherung konnte - nicht zuletzt aufgrund der Proteste der Datenschützer - erfolgreich verhindert werden.

Allerdings gibt es nun auf europäischer Ebene Bestrebungen, eine Verpflichtung zur flächendeckenden und anlassunabhängigen Speicherung von Daten auf Vorrat einzuführen. Gegen diese Verpflichtung habe ich mich am 25. Juni 2004 in einer gemeinsamen Pressemitteilung mit dem Bundesbeauftragten und den anderen Landesbeauftragten für den Datenschutz gewandt. Es bleibt zu hoffen, dass diese datenschutzrechtlichen Bedenken Gehör finden und eine solche Verpflichtung erfolgreich abgewehrt werden kann.

Verkehrsdaten werden im Regelfall vollständig gespeichert: Im Regelfall werden Verkehrsdaten (im TKG a. F. noch als Verbindungsdaten bezeichnet) nunmehr unverkürzt und vollständig gespeichert. Die vollständige Speicherung soll im Fall von der Reklamation der Rechnung einen Rückgriff auf die angerufene Nummer ermöglichen. Allerdings steht dem Kunden weiterhin ein Wahlrecht zu: Er kann auch eine um die letzten Ziffern verkürzte Speicherung oder die sofortige Löschung seiner Verkehrsdaten mit Versendung der Rechnung wählen. Wird von dem Wahlrecht kein Gebrauch gemacht, wird die Zielnummer unverkürzt gespeichert.

2.2 Erlaubnis erweiterter Datenbeschaffung durch die GEZ

Am 8. Oktober 2004 haben die Ministerpräsidenten der Länder den 8. Rundfunkänderungsstaatsvertrag unterzeichnet. Seitens der bremischen Senatskanzlei wurde ich von dieser Änderung nicht unterrichtet, obwohl hierzu eine gesetzliche Verpflichtung besteht. Dies ist bedauerlich, da mir hierdurch die Möglichkeit genommen wurde, frühzeitig datenschutzrechtliche Bedenken anzumelden.

Aus datenschutzrechtlicher Sicht ist der neue § 8 Abs. 4 Rundfunkgebührenstaatsvertrag (RGbStV) besonders relevant. Hiernach darf die GEZ im Auftrag der Rundfunkanstalten personenbezogene Daten entsprechend § 28 Bundesdatenschutzgesetz (BDSG) verarbeiten. Diese Regelung soll die Beschaffung von Adressen bei kommerziellen Adresshändlern durch die GEZ legitimieren. Die GEZ nutzt diese Daten für flächendeckende Mailing-Aktionen. Im Jahr 2003 wurden insgesamt 18,7 Millionen Briefe im Rahmen des Mailings versandt, wobei allerdings die Daten nicht nur von Adresshändlern, sondern auch von den Einwohnermeldeämtern stammten. Da die von den Adresshändlern gelieferten Daten nicht immer korrekt oder aktuell sind, kann es auch schon mal passieren, dass auch Haustiere (z. B. die Familienratte) oder Verstorbene angeschrieben werden.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt dafür eingesetzt, bei der Finanzierung des öffentlichen Rundfunks die Grundsätze der Datenvermeidung und Datensparsamkeit stärker zu berücksichtigen. Die neu geschaffene Regelung steht im krassen Widerspruch zu diesen Prinzipien und ist zudem völlig systemfremd. Die Regelung soll bezwecken, dass die Rundfunkanstalten und die GEZ wie privatwirtschaftliche Unternehmen agieren können. Dieses lässt sich aber nicht mit datenschutzrechtlichen Grundsätzen vereinbaren. Während öffentlich-rechtliche Institutionen personenbezogene Daten nur verarbeiten dürfen, wenn dies zur Erfüllung ihrer gesetzlichen Aufgabe erforderlich ist, ist die Datenverarbeitung der im Wettbewerb stehenden privatwirtschaftlichen Unternehmen vom Prinzip der Vertragsfreiheit geprägt. Die öffentlich-rechtlichen Rundfunkanstalten stehen hinsichtlich des Gebühreneinzugs in keinem Wettbewerb mit anderen Rundfunkveranstaltern. Außerdem haben die Rundfunkanstalten auch noch zusätzlich ihren Bonus als öffentliche Stelle, wonach sie Daten aus Melderegistern nutzen dürfen. Beide Befugnisse zusammen stellen sich unverhältnismäßig dar und sind damit verfassungsrechtlich bedenklich. In der Datenerhebung hinter dem Rücken des Betroffenen liegt ein erheblicher Eingriff in sein Recht auf informationelle Selbstbestimmung.

Diese Kritik haben die Datenschutzbeauftragten der Länder Berlin, Brandenburg, Bremen, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Sachsen und Schleswig-Holstein auch in einer gemeinsamen Presseerklärung vom 8. November 2004 bekundet, die auf meiner Homepage zu finden ist.

2.3 Beratung bei der Novellierung des Bremischen Landesmediengesetzes

Anders als beim 8. Rundfunkgebührenstaatsvertrag (vgl. Ziff. 2.2 dieses Berichts) wurde ich über die beabsichtigte Novellierung des Landesmediengesetzes (BremLMG) frühzeitig von der Senatskanzlei unterrichtet. Es sollte im Rahmen der Novellierungsbestrebungen geprüft werden, ob Regelungsbereiche im Landesmediengesetz entfallen können, wenn die Vorschriften des Rundfunkstaatsvertrags ausreichend sind. Ich habe in meiner Stellungnahme gegenüber der Senatskanzlei von einer Streichung von Regelungen im Landesmediengesetz abgeraten, da es sich entweder um unverzichtbare Regelungen handelt oder sie der Klarheit dienen. Zudem habe ich noch auf Anpassungsbedarf an das neue Bundesdatenschutzgesetz (BDSG) hingewiesen. Meine Anregungen wurden seitens der Senatskanzlei berücksichtigt. Das Landesmediengesetz wurde am 11. Mai 2004 geändert (vgl. Brem.GBl. 2004, S. 203) und trat am Tag nach seiner Verkündung in Kraft.

3. Datenschutz durch Technikgestaltung und -bewertung

3.1 Virtuelle Poststelle

Das Konzept der virtuellen Poststelle beschreibt ein zentrales System, das die sichere elektronische Kommunikation innerhalb der Behörden, zwischen Behörden und mit externen Kommunikationspartnern unterstützen soll. Als zentrales Security-Gateway stellt sie Funktionen zur Ent- und Verschlüsselung, Signaturprüfung- und Signaturerstellung sowie zur Authentifizierung bereit. E-Mail- und Webanwendungen können diese Funktionen nutzen.

Der Senator für Finanzen hat ein Pilotprojekt gestartet, an dem meine Dienststelle mit folgender Zielsetzung teilgenommen hat:

- Prüfung der Einsatzmöglichkeiten in eigenen Geschäftsfeldern
- Begleitung der Erstellung eines „Musterkonzeptes“ zum Datenschutz

Während der Pilotphase wurden zunächst die im Rahmen der Version für das elektronische Verwaltungs- und Gerichtspostfach (EVGP) zur Verfügung gestellten Funktionen im Echteinsatz getestet.

Dazu gehörten beispielsweise die Sendefunktion mit mehreren Varianten und Anhängen ohne Signatur sowie mit fortgeschrittener oder qualifizierter Signatur. Darüber hinaus wurden u. a. die Signaturauswahl oder der Umgang mit zu nutzenden Zertifikaten getestet. Neben dem Funktionstest wurden weitere Anforderungen an eine Standardversion für den Einsatz in der allgemeinen Verwaltung entwickelt.

Mit der Erstellung des Datenschutzkonzeptes ist begonnen worden. Dadurch, dass die virtuelle Poststelle eine zentrale Anwendung ist, die in einem heterogenen Umfeld genutzt werden soll, müssen verschiedene Anwendungs- und Funktionsebenen im Konzept berücksichtigt werden.

Dies könnte beispielsweise durch die Erstellung von Teilkonzepten mit folgenden Inhalten ermöglicht werden:

- Virtuelle Poststelle (VPS): Hier ist zu unterscheiden zwischen Datensicherungsmaßnahmen zum Schutz der VPS (Schutzobjekte sind hier Dateien und Systeme zum Betrieb der VPS) und den Datensicherungsmaßnahmen in der VPS (Schutzobjekte sind hier die Kommunikationsdaten)
- Dienste (Authentifizierung, Vertraulichkeit, Integrität, Verbindlichkeit, Monitoring/Auditing)
- Verarbeitung der Daten in den einzelnen Dienststellen

Die Struktur einer anwendungsfähigen Datenschutzkonzeption wird im nächsten Jahr noch in der Projektgruppe diskutiert werden.

3.2 Mobiler Fernzugriff für Führungskräfte auf das BVN

Im vergangenen Jahr habe ich über den Fernzugriff für Führungskräfte im Rahmen eines Pilotprojektes des Senators für Finanzen berichtet (vgl. 26. JB, Ziff. 3.3). Stand der Technik war damals die Einwahl von fest vereinbarten Standorten in das Netz des Senators für Finanzen.

In diesem Jahr wurde die Zugriffsmöglichkeit auf wechselnde Standorte (z. B. Hotels, Konferenzräume etc.) erweitert. Der Zugriff über das Bremer Verwaltungsnetz in das lokale Netz des Senators für Finanzen erfolgt dabei vom Notebook über das Internet. Die damit verbundenen Gefahrenpotentiale sind wesentlich höher als bei der Herstellung der Verbindung zum Bremer Verwaltungsnetz von fest vereinbarten Standorten über ISDN-Leitungen. Davon geht auch der Senator für Finanzen in seinem mir zur Verfügung gestellten Abschlussbericht aus. In seiner Konzeption wird deshalb ein hoher Standard an Techniken zur Datensicherheit vorgesehen. Die Datensicherheit wird unter Einbeziehung einer Risikoanalyse auf der Ebene von vier für die Kommunikation wesentlichen Komponenten betrachtet, nämlich der entfernte Zugriffspunkt (Notebook), die öffentliche Vermittlung (für den mobilen Zugriff auf das Internet), das Bremer Verwaltungsnetz und das lokale Netz der Dienststelle.

Für den mobilen Zugriff ist die Absicherung der Notebooks sowie die Sicherung des Datentransfers über das Internet von zentraler Bedeutung. Hierfür sind komplexe Sicherheitstechnologien, u. a. die Installation einer Firewall auf den Notebooks, Verschlüsselung der Festplatte, die Installation einer Sicherheitssoftware sowie der Einsatz eines VPN-Clients. Der VPN-Client (VPN = Virtual Private Network) baut eine sichere Verbindung unter Verwendung von Zertifikaten mit dem VPN-Server der BreKom (Übergang in das bremische Verwaltungsnetz) auf. Dieser Aufbau erfolgt über den IPSec-Standard (Internet Protocol Security). Dieser Standard ist ein Sicherheitsstandard, dessen Ziel die Informationsvertraulichkeit, Authentizität und Datenintegrität beim Datentransfer in unsicheren Netzen wie dem Internet ist.

Die aufgrund der Risikoanalyse getroffenen Maßnahmen befinden sich auf dem Stand der Technik und sind deshalb von mir als angemessen im Sinn des Bremischen Datenschutzgesetzes (§ 7 Abs. 3) bewertet worden.

Es besteht dennoch ein nicht auszuschließendes Restrisiko, z. B. sind Anwenderfehler, Fehler in der Sicherheitssoftware und deren Konfiguration, nicht kalkulierbare Angriffe aus dem Internet und die Komplexität der Sicherheitsstruktur selbst.

Die Komplexität der technischen Maßnahmen ist nicht mehr nur in einzelnen Funktionen, sondern nur noch vor dem Hintergrund der Wechselwirkungen untereinander und innerhalb bestimmter Umgebungen wie beispielsweise dem Internet zu verstehen. Das erfordert eine hohe, ständig wachsende Qualifikation für den Bereich der Administration, aber auch für die Anwender. Um z. B. mit einem durch eine Firewall (Programm zum Schutz von Angriffen aus dem Internet) geschützten Laptop im Internet zu arbeiten, ist es erforderlich, Meldungen der Firewall zu verstehen. Dies setzt zumindest ein Grundwissen in Netztechnologie voraus.

Darüber hinaus wächst die Verteilung von Verantwortlichkeiten. In diesem Projekt wird das gesamte Sicherheitsniveau aus verschiedenen Bereichen und deren Zusammenspiel gebildet. Verantwortlich für seine Daten ist der Senator für Finanzen. An der faktischen Verantwortung sind aber bereits mehrere Stellen beteiligt. Dazu gehören neben der BreKom (verantwortlich für die Sicherheit im Bremer Verwaltungsnetz) auch der Anwender und letztendlich auch die Softwarefirmen, deren Sicherheitstechnologie genutzt wird und auf deren Wirkmechanismen vertraut wird.

Die Abhängigkeit der Sicherheit komplexer Systeme von den Wechselwirkungen effektiver Einzelmaßnahmen setzt auch ein hohes Maß an Kommunikation der faktisch Verantwortlichen voraus. Hier erhöhen sich die Anforderungen an Kommunikationsfähigkeit und -bereitschaft. Eine große Herausforderung für den Datenschutz wird es zukünftig sein, die Verantwortung nach § 2 Abs. 3 Nr. 1 BremDSG in komplexer werdenden Systemen klar zuordnen zu können.

3.3 Prüfungen von Funk-LAN-Verbindungen in der Verwaltung

3.3.1 Amt für Jugend und Familie – Stadtteilbüro Nord

Im letzten Jahr berichtete ich über die Einrichtung einer Funkstrecke zwischen einer Ausgliederung der Zweigstelle des Stadtteilbüros Nord, das über eine Standleitung an das Subnetz des Amtes für Jugend und Familie angebunden ist (vgl. 26. JB, Ziff. 9.3). Die zwischen dem Stadtteilbüro Nord und der Zweigstelle implementierte Funkstrecke besteht aus zwei Access-Points (Funkzellen), die im LAN-to-LAN-Betriebsmodus eingesetzt werden, also als Bridge fungieren (Wireless Bridging).

Aufgrund des höheren Gefährdungspotentials gegenüber drahtgebundenen Netzen in Bezug auf die Zugangs- und Abhörsicherheit (unbeabsichtigtes Einloggen in das Funk-LAN und Mithören des Funk-LAN-Datenverkehrs) hatte ich gegenüber dem Amt für Jugend und Familie diesem Gefährdungspotential entsprechende und die Sensibilität der Daten berücksichtigende Sicherheitsanforderungen formuliert. In diesem Jahre habe ich deren Umsetzung überprüft und konnte feststellen, dass meine Anforderungen auf hohem technischen Niveau umgesetzt worden sind. Dies wurde insbesondere durch die Verwendung zusätzlicher Sicherheitslösungen erreicht.

Der Schutz der mit dem Funknetz gekoppelten lokalen Netze wurde beispielsweise durch folgende Maßnahmen implementiert:

- Abschaltung der SSID (Service-Set-Identity)-Broadcast. Damit wird erreicht, dass dieses Netz seine Kennung nicht mehr bekannt gibt und diese somit auch nicht durch entsprechende Programme ausgeforscht werden kann.
- Bildung eines Transfernetzes für den Funkverkehr
- Aufbau eines VPN-Tunnels auf der Funkstrecke zwischen den Routern der jeweils lokalen Netzwerke. Damit wird beim Verbindungsaufbau ein kryptografischer Tunnel (hier basierend auf dem Standard IPSec – Internet Protokoll Security) zwischen den Routern der lokalen Netze erzeugt. Die Vertraulichkeit der Information, deren Authentizität und die Datenintegrität sind somit angemessen gewährleistet
- Administration der Access-Points nur über drahtgebundene Übertragungswege
- Einsatz von Firewalls zur Filterung des Datenverkehrs

3.3.2 Helene-Kaisen-Haus

Das Helene-Kaisen-Haus (eine Einrichtung für sozialpädagogische Dienstleistungen in Bremerhaven) hat Arbeitsplätze, die sich außerhalb der Einrichtung befinden, über eine Funkverbindung mit dem Netzwerk der Stammeinrichtung verbunden. Grundlegend für die Installation waren die Sicherheitsanforderungen, die ich bereits gegenüber dem Amt für Jugend und Familie formuliert hatte.

Eine von mir durchgeführte Prüfung bestätigte ebenfalls die korrekte Installation.

3.3.3 Ausländerbeauftragte

Ich führe von Zeit zu Zeit sowohl in Bremen als auch in Bremerhaven so genanntes Wardriving durch. Wardriving dient dazu, Funknetze aufzuspüren. Dazu wird lediglich ein handelsübliches Notebook mit einer WLAN-Funknetz-Karte und entsprechender Software, die frei im Internet verfügbar ist, benötigt. Entsprechend ausgerüstet, können während des Fahrens oder Gehens durch die Stadt Funknetze aufgespürt werden. Ich suche dabei nach Funknetzen, die ich direkt den betreibenden Einrichtungen zuordnen kann und prüfe, ob Sicherungsmaßnahmen für das entsprechende Funknetz vorgenommen worden sind. Dabei fiel mir im Sommer ein Funknetz mit dem Namen „Ausländerbeauftragte“ auf. Die von mir während des Wardriving gefundenen zugehörigen Daten ließen den Schluss zu, dass möglicherweise nicht ausreichende Sicherungsmaßnahmen getroffen wurden, um dieses Funknetz gegenüber unbefugter Einfluss- oder Kenntnisnahme abzusichern. Ich habe auf eine weitergehende Analyse des Netzes verzichtet, umgehend Kontakt zur Ausländerbeauftragten aufgenommen und das Funknetz einer Prüfung unterzogen. Dabei konnte ich feststellen, dass das Funknetz völlig ohne Sicherungsmaßnahmen betrieben wurde. Zu bemängeln war u. a., dass der Name des Funknetzes, die sogenannte SSID, sprechend („Ausländerbeauftragte“) war, das Broadcast dieser SSID nicht unterdrückt wurde und dass keine Verschlüsselung der übertragenen Daten stattfanden. Für den technischen Betrieb dieses Netzes war zum Zeitpunkt der Prüfung die Abteilung „Technikunterstützte Informationsverarbeitung - Netzadministration des Sozialressorts“ zuständig. Von dort wurde mir während der Prüfung ein Schreiben eines externen Dienstleistungsunternehmens, das mit der Realisierung der Funkvernetzung bei der Ausländerbeauftragten beauftragt war, vorgelegt. In diesem wurde versichert, dass ausreichende Maßnahmen zur Absicherung des Funknetzes ergriffen wurden. Daraufhin habe ich zusammen mit den Mitarbeitern der Abteilung „Technikunterstützte Informationsverarbeitung – Netzadministration des Sozialressorts“ das Funknetz der Ausländerbeauftragten nochmals die technischen Sicherungsmaßnahmen geprüft und konnte aufzeigen, dass das Netz entgegen der Aussage in dem Schreiben völlig ungeschützt betrieben wurde. Das Sozialressort hat dann mir gegenüber Sofortmaßnahmen zur Absicherung des Netzes angekündigt. Diese sind unverzüglich umgesetzt worden.

4. Bremische Bürgerschaft – Die Arbeit des Rechtsausschusses

4.1 Ergebnisse der Beratung des 26. Jahresberichts

Bericht und Antrag des Rechtsausschusses vom 25. Februar 2005 zum 26. Jahresbericht des Landesbeauftragten für den Datenschutz (Drs. 16/189) und zur Stellungnahme des Senats vom 31. August 2004 (Drs. 16/379)

I. Bericht

Die Bürgerschaft (Landtag) überwies in ihrer Sitzung am 5. Mai 2004 den 26. Jahresbericht des Landesbeauftragten für den Datenschutz und in ihrer Sitzung am 7. Oktober 2004 die Stellungnahme des Senats an den Rechtsausschuss zur Beratung und Berichterstattung.

Der Ausschuss stellte im Rahmen der Behandlung des 26. Jahresberichtes und der Stellungnahme des Senats bei den nachfolgend aufgeführten Punkten Beratungs- und Handlungsbedarf fest:

Ziffer 6.3.2 - Bürger-Service-Center

Ziffer 6.3.5 - Waffenrecht

Ziffer 7.3 - Veröffentlichung der Insolvenzbekanntmachungen im Internet

Ziffer 8.2.2 - Mammographie-Screening

Ziffer 10.1.2 - Vergleichsarbeiten an Bremer Schulen - VERA -

Ziffer 13.2 - ELSTER (Elektronische Steuererklärung).

In seinen Sitzungen am 24. November 2004 und 19. Januar 2005 erörterte der Ausschuss die beratungsbedürftigen Punkte mit dem Landesbeauftragten für den Datenschutz unter Hinzuziehung der Vertreter der betroffenen Ressorts. Die abschließende Beratung fand in der Sitzung am 16. Februar 2005 statt.

Auf die in der Stellungnahme des Senats erfolgte Ankündigung, der Senat werde über Form und Funktion der Datenschutzberichte mit den in Bremen mit den Belangen des Datenschutzes befassten Stellen in eine Diskussion zur Zukunft des Jahresberichts eintreten, stellte der Ausschuss fest, dass der Landesbeauftragte für den Datenschutz nach dem geltenden Recht Art und Umfang seines Berichtes selbst bestimme und der Senat nicht befugt sei, ihm diesbezügliche Vorgaben zu machen. Im Sinne einer besseren Lesbarkeit regte der Ausschuss an, die streitigen Punkte mit Diskussions- und Handlungsbedarf gesondert auszuweisen. Der Ausschuss hält eine zeitnahe Berichterstattung - zum Beispiel auch wegen neuer technischer Entwicklungen - auch weiterhin für unverzichtbar.

Zu den einzelnen Punkten nimmt der Rechtsausschuss wie folgt Stellung:

Bürger-Service-Center (Ziffer 6.3.2): Nach §§ 7 und 8 Bremisches Datenschutzgesetz ist die verantwortliche Stelle verpflichtet, für jedes automatisierte Verfahren, mit dem personenbezogene Daten verarbeitet werden, in einer Beschreibung bestimmte Abläufe und Zugriffsmöglichkeiten auf die Daten festzulegen und ein Datenschutzkonzept zu entwickeln. Für das seit Ende 2002 in Betrieb befindliche Bürger-Service-Center fehlt bislang ein verbindliches Datenschutzkonzept für eine korrekte Verarbeitung der Daten und Implementierung der Datenschutzgrundsätze in dem umfangreichen Verfahren.

Der Senator für Inneres und Sport erläuterte, dass das Datenschutzkonzept unter anderem aus Gründen nicht hinreichender personeller Kapazitäten bislang nicht habe erstellt werden können, ein Datenmissbrauch in jedem Fall aber ausgeschlossen sei. Angesichts der im Verlauf des Jahres 2005 anstehenden Veränderungen für Großverfahren wie Kfz-Zulassungs-, Melde- und Gewerbeverfahren kündigte der Senator für Inneres und Sport die Vorlage eines Datenschutzkonzeptes bis voraussichtlich Ende 2005 an.

Der Ausschuss bat den Senator für Inneres und Sport für seine Ausschusssitzung am 19. Januar 2005 um die Vorlage eines Terminplanes unter Angabe des Zeitpunktes einer Vorlage des Rahmenkonzeptes sowie der Einführung der neuen Verfahren - unter anderem in den Bereichen Gewerbe- und Kfz-Angelegenheiten. Der Senator für Inneres und Sport legte den erbetenen Zeitplan dem Ausschuss in seiner Sitzung am 16. Februar 2005 vor. Danach wurden die Arbeiten am Datenschutzkonzept zwischenzeitlich aufgenommen.

Das Datenschutzkonzept für das Bürger-Service-Center setzt sich aus einzelnen Modulen zusammen:

Für die Bereiche Kfz-Zulassung, Besuchereinladung, Fischereiangelegenheiten, Antragsannahme für Berechtigungsscheine, Wohngeld und Erziehungsgeld sowie Internet, räumliche Rahmenbedingungen wird ein Abschluss der Arbeiten bis Mitte März 2005 angekündigt; für den Bereich Netzwerk und Zugriffsschutz ist der Abschluss bis zum 30. Juni 2005 geplant. Nach der Einführung neuer Programme werden die Module Gewerbe bis Herbst 2005 und Meldewesen bis Februar 2006 abgeschlossen sein.

Der Ausschuss nimmt den vorgelegten Zeitplan zur Kenntnis und stellt fest, dass das Datenschutzkonzept dem Grunde nach bereits im Rahmen der Vorbereitung der Inbetriebnahme der automatisierten Datenverarbeitung spätestens Ende 2002 hätte entwickelt werden müssen.

Waffenrecht (Ziff. 6.3.5): Für das DV-Verfahren zur Umsetzung des zum 1. April 2003 in Kraft getretenen neuen Waffengesetzes existierte ungeachtet mehrfacher Aufforderungen des Landesbeauftragten für den Datenschutz noch kein Datenschutzkonzept bei der im Stadtamt angesiedelten Waffenstelle.

Der Senator für Inneres und Sport wies den Ausschuss darauf hin, dass in der Waffenstelle derzeit lediglich eine elektronische Aktenverwaltung auf einem internen Netzwerk innerhalb des Sachgebietes stattfinde, die zuvor auf Karteikarten erledigt worden sei. Das geschlossene Verfahren stehe lediglich den Mitarbeitern der Waffenbehörde, nicht aber anderen Mitarbeitern des Stadtamtes zur Verfügung und beinhalte keine Schnittstellen nach außen. Die Definition der Schnittstellen sei für Frühjahr 2005 geplant. Das Datenschutzkonzept könne erst nach Definition der Schnittstellen und Abschluss des gesamten Verfahrens vorgelegt werden.

Der Ausschuss akzeptierte den vom Senator für Inneres und Sport in der Sitzung am 24. November 2004 vorgestellten Zeitplan nicht und bat stattdessen um Vorlage des Datenschutzkonzeptes bis zum 31. Dezember 2004.

In der Ausschusssitzung am 19. Januar 2005 berichtete der Senator für Inneres und Sport, dass der Entwurf eines Datenschutzkonzeptes „Automatisierte Datenverarbeitung in der Waffenverwaltung

(Waffenregister)“ seit dem 30. Dezember 2004 vorliege und sich in der Abstimmung mit dem Landesbeauftragten für den Datenschutz befinde.

Der Ausschuss stellt fest, das ein Datenschutzkonzept bereits bei Einführung des Verfahrens hätte vorliegen müssen und bedauert, dass ein abgestimmtes Konzept immer noch nicht vorliegt. Der Ausschuss nimmt zur Kenntnis, dass nunmehr ein Entwurf erstellt wurde und geht davon aus, dass die endgültige Klärung zu den Bereichen Datenbank, Netzwerksicherheit und Zugriffsrechte kurzfristig erfolgen wird.

Veröffentlichung der Insolvenzbekanntmachungen im Internet (Ziffer 7.3): Seit Herbst 2003 veröffentlichen die Insolvenzgerichte in Bremen und Bremerhaven die öffentlichen Bekanntmachungen im Internet auf der Website „www.insolvenzbekanntmachungen.de“ unter der federführenden Betreuung des Landes Nordrhein-Westfalen. Diesem Verfahren liegt eine Verwaltungsvereinbarung zwischen vierzehn Bundesländern zugrunde, nach der das Register der Insolvenzbekanntmachungen auf einer Website des Landes Nordrhein-Westfalen veröffentlicht und gepflegt wird. Die Einzelheiten der Veröffentlichung werden in § 9 Abs. 2 S. 3 Nr. 3 Insolvenzordnung (InsO) sowie der Insolvenzbekanntmachungsverordnung (InsoBekV) geregelt. Nach diesen Vorschriften ist zu gewährleisten, dass die veröffentlichten Daten durch Dritte nicht elektronisch kopiert werden können, um das Anlegen privater Insolvenzverzeichnisse zu vermeiden. Für Schuldner besteht dadurch die Gefahr, gegebenenfalls noch lange Zeit nach Ablauf ihrer Insolvenz in privat angefertigten Schuldnerverzeichnissen gespeichert zu bleiben.

Der Gesetzgeber hat angesichts dieser Gefahrenlage gesetzliche Regelungen geschaffen. Hierdurch soll einer Speicherung und Verbreitung durch Dritte entgegen gewirkt werden. § 9 Abs. 2 S. 3 Nr. 3 InsO und § 2 Abs. 1 Satz 3 InsoBekV verlangen, dass die Veröffentlichungen nach dem Stand der Technik durch Dritte nicht kopiert werden können. Auf der von den Ländern genutzten Internetseite wird der gesetzlich geforderte Kopierschutz nicht eingehalten. Auf der ersten Ergebnisebene der über das Internet für jedermann abrufbaren Datei ist nur ein ungenügender Kopierschutz vorhanden. Sie enthält Namen, Sitz bzw. Wohnsitz, Aktenzeichen und das Datum der Erstveröffentlichung. Diese Daten lassen sich sowohl mit der Kopierfunktion „copy and paste“ als auch in Listenform als Datei speichern. Auf der zweiten Ergebnisebene, welche die weiteren Angaben der Insolvenzveröffentlichung beinhaltet, wird der Kopierschutz nur durch ein Java-Skript hergestellt. Dies kann ohne besonderen Aufwand leicht umgangen werden, da die Datei als temporäre Internetdatei auf dem Rechner abgelegt wird.

Das vom Landesbeauftragten für den Datenschutz entwickelte Verfahren für einen Kopierschutz ist geeignet zu verhindern, dass die Daten aus der nordrhein-westfälischen Internetbekanntmachung von Dritten gespeichert und elektronisch ausgewertet werden können. Der Senator für Justiz und Verfassung teilte dem Ausschuss mit, dass die vom Landesbeauftragten für den Datenschutz unterbreiteten Anregungen Anfang 2004 an Nordrhein-Westfalen weitergeleitet wurden. Das Land Bremen selbst habe jedoch keinen unmittelbaren Einfluss auf das Verfahren.

Der Landesbeauftragte für den Datenschutz verdeutlichte, dass nach § 3 InsoBekV auch die in einem elektronischen Informations- und Kommunikationssystem erfolgten Veröffentlichungen von Daten aus

einem Insolvenzverfahren einschließlich des Eröffnungsverfahrens spätestens einen Monat nach der Aufhebung oder der Rechtskraft der Einstellung des Insolvenzverfahrens zu löschen seien. Diese Löschungsfristen können umgangen werden, wenn kein ausreichender Kopierschutz unter Verwendung des jeweils modernsten Verfahrens zur Verhinderung des Kopierens der Daten durch Dritte bestehe.

In der Beratung des Ausschusses sagte der Vertreter des Senator für Justiz und Verfassung zu, dem Justizministerium von Nordrhein-Westfalen das dem Ausschuss vorgestellte Konzept des Landesbeauftragten für den Datenschutz zum Kopierschutz mit der Bitte um Stellungnahme zuzuleiten und dem Ausschuss zu berichten.

Der Ausschuss wird sich mit der Angelegenheit in seiner Sitzung am 13. April 2005 erneut befassen.

Mammographie-Screening (Ziffer 8.2.2): Der Landesbeauftragte für den Datenschutz erläuterte die Problemstellung: Nach einer Auswertung der Aufnahmen des Mammographie-Zentrums würden Frauen mit dem Verdacht auf einen Brustkrebs-Befund erneut zur Untersuchung eingeladen. Da dies wie bei der ersten Untersuchung jeweils straßenweise geschehe, hätten sich einige Frauen darüber beschwert, in der Wartezone auf Nachbarinnen zu treffen. Um den Belangen der Frauen Rechnung zu tragen, forderte der Landesbeauftragte für den Datenschutz die Änderung des Verfahrens zur Einladung der Frauen.

Der Ausschuss hält es für dringend geboten, angesichts der bei den betroffenen Frauen ohnehin bestehenden psychischen Belastungen eine die Persönlichkeitsrechte der Frauen berücksichtigende Verfahrensänderung vorzunehmen, die gewährleisten müsse, dass bei gegebenenfalls erforderlich werdenden Nachuntersuchungen die Einladungen nicht nach Straßen geordnet erfolgen.

Der Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales sagte in der Ausschusssitzung am 24. November 2004 zu, mit dem Nachfolger der Einrichtung gegebenenfalls räumliche Regelungen zu treffen und eventuell auch das Einladungsverfahren für die zweite Abklärungsdiagnostik zu verändern.

Der Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales teilte dem Ausschuss in seiner Sitzung am 16. Februar 2005 mit, dass die Modellphase am 31. März 2005 auslaufe und ab 1. April 2005 das Mammographie-Screening im Rahmen der Regelversorgung durch niedergelassene Ärzte durchgeführt werde. Eine Änderung des Verfahrens müsse durch den programmverantwortlichen Arzt erfolgen, insoweit könne das Ressort keine verbindlichen Vorgaben machen.

Der Ausschuss nimmt zur Kenntnis, dass der Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales die durchführenden Ärzte auf die Problematik hinweisen und um entsprechende Änderungen für das Einladungsverfahren in der Abklärungsdiagnostik bitten wird.

Vergleichsarbeiten an Bremer Schulen (VERA) (Ziffer 10.1.2): Aufgrund des bei VERA recht kurzen Vorlaufes erfolgte die Unterrichtung des Landesbeauftragten für den Datenschutz erst zu einem Zeitpunkt, als das Projekt in den Schulen angelaufen war und die Daten bereits erhoben wurden. So konnten die datenschutzrechtlichen Hinweise des Landesbeauftragten durch den Senator für Bildung und Wissenschaft nicht mehr umgesetzt werden.

In diesem Zusammenhang wies der Landesbeauftragte für den Datenschutz darauf hin, dass es in der Vergangenheit wiederholt vorgekommen sei, dass der Senator für Bildung und Wissenschaft den Datenschutzbeauftragten nicht frühzeitig über anstehende Projekte unterrichtet habe - so unter anderem beim Projekt „Schule macht sich stark“. Bei rechtzeitiger Beteiligung des Datenschutzbeauftragten wäre in diesem Falle beispielsweise die zugesicherte Anonymität zu gewährleisten gewesen.

Der Senator für Bildung und Wissenschaft erläuterte im Ausschuss, dass der Datenschutzbeauftragte bei VERA lediglich einen Satz im Anschreiben an die Eltern beanstandet habe und der Datenschutz im Übrigen gewährleistet gewesen sei. Die Verarbeitung der Daten habe Rückschlüsse auf bestimmte Personen nicht erlaubt. Eine Verletzung des Datenschutzes an sich sei nicht erfolgt, lediglich der Zeitpunkt der Benachrichtigung sei wegen des kurzen Vorlaufes sehr kurzfristig gewesen.

Angesichts der unterschiedlichen Auffassungen der Datenschutzbeauftragten der einzelnen Bundesländer zu den Elternanschreiben sei bei überregionalen Projekten eine Absprache der Datenschutzbeauftragten untereinander erforderlich. Zur Sicherstellung der Durchführung auch kurzfristiger Projekte regte der Senator für Bildung und Wissenschaft an, eine Vereinfachung durch eine regelhafte Absprache zu erreichen, indem man mit dem Landesbeauftragten für den Datenschutz abgestimmte grundsätzliche Hinweise entwickele, die der Senator für Bildung und Wissenschaft bei Bedarf den an die Eltern gerichteten Anschreiben beifügen könne. So werde vermieden, dass jedes einzelne Verfahren mit erheblichem Zeitaufwand neu abgestimmt werden müsse.

Der Landesbeauftragte für den Datenschutz wies darauf hin, dass nach dem bremischen Schuldatenschutzgesetz bestimmte Daten aus dem sozialen Umfeld der Schüler nur mit der freiwilligen Zustimmung der Eltern erfasst werden, da eine zwingende Zustimmung der Eltern nicht vorgesehen sei. Bei den Elternanschreiben zur Einholung der Einwilligung werden jeweils auch Hintergrundinformationen zu den einzelnen Projekten geliefert, so dass die vom Senator für Bildung und Wissenschaft angeregte Formalisierung auf Zweckmäßigkeit geprüft werden müsse.

Der Ausschuss geht davon aus, dass der Landesbeauftragte für den Datenschutz bei künftigen Projekten entsprechend frühzeitig unterrichtet wird.

ELSTER (Elektronische Steuererklärung) (Ziffer 13.2): Für das bereits im Echtbetrieb laufende Verfahren ELSTER konnte bei einer Prüfung des Verfahrens durch den Landesbeauftragten für den Datenschutz kein Datenschutzkonzept vorgelegt werden.

Der Senator für Finanzen stellte den Programmablauf von ELSTER dar und räumte gegenüber dem Ausschuss ein, dass gegenwärtig kein bremisches Datenschutzkonzept existiere. Die Daten der Steuerpflichtigen laufen verschlüsselt bei den Clearingstellen in Düsseldorf und München auf. Diese Stellen werden von den dortigen Datenschutzbeauftragten begutachtet. Auch die Software der Server der Landeskopfstelle in Bremen werde von den Clearingstellen gepflegt. Das Steuerprogramm für die Bürger werde im ELSTER-Verbund entwickelt. Deshalb habe Bremen darauf keinen technischen Einfluss, ebenso wenig wie auf andere Sicherheitsvorkehrungen oder Verschlüsselungsverfahren. Aus diesem Grunde habe der Senator für Finanzen ein bremisches Datenschutzkonzept bislang nicht für erforderlich gehalten. Lediglich für die nach der Entschlüsselung erfolgende Übertragung zum

Rechenzentrum seien Regelungen durch ein bremisches Datenschutzkonzept zugänglich. Der Senator für Finanzen sagte in der Sitzung des Rechtsausschusses am 24. November 2004 die Entwicklung eines eigenen Datenschutzkonzeptes zu.

In der Sitzung des Ausschusses am 19. Januar 2005 teilte der Landesbeauftragte für den Datenschutz dem Ausschuss mit, dass der Senator für Finanzen zwischenzeitlich ein Datenschutzkonzept vorgelegt habe, das den Anforderungen genüge.

Der Ausschuss begrüßt die Vorlage des Datenschutzkonzeptes zum Bereich der Elektronischen Steuererklärung.

II. Antrag

Die Bürgerschaft (Landtag) möge beschließen:

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

4.2 Weitere Themen der Beratungen im Rechtsausschuss

Über die unter Ziff. 4.1 dargestellten Ergebnisse hinaus hat sich der für den Datenschutz zuständige Parlamentsausschuss u. a. auch mit den nachfolgenden Themen beschäftigt:

- Zuständigkeit für die Datenschutzkontrolle bei Radio Bremen
- Übermittlung von Daten über die Halter von Kampfhunden für Zwecke der Besteuerung
- Einführung der elektronischen Arbeitszeiterfassung in der bremischen Verwaltung
- DNA-Reihenuntersuchung in Bremerhaven
- Polizeiliches Vorgangsbearbeitungssystem NIVADIS
- Auswirkungen des Urteils des Bundesverfassungsgerichts vom 3. März 2004 zur akustischen Wohnraumüberwachung
- Erhebung und weitere Verarbeitung von personenbezogenen Daten im Rahmen von Hartz IV
- Gewährleistung des Datenschutzes bei der Umsetzung des ISPS-Codes
- Informationsaustausch über Kampfhundehalter zwischen Polizei und Stadtamt

Die Sitzungen des Rechtsausschusses sind in der Regel öffentlich.

5. Personalwesen

5.1 Aufbau eines Mitarbeiterportals

Im Rahmen des Gesamtprojektes „Virtuelles Personalbüro“ hat der Senator für Finanzen eine Softwarelösung entwickelt, die u. a. den Aufbau eines Mitarbeiterportals (MiP) beinhaltet. Aus datenschutzrechtlicher Sicht bedeutsam ist, dass durch eine erweiterte Anwendung des PuMa-Verfahrens (Personalverwaltung und -management) den Beschäftigten der bremischen Verwaltung direkt von ihrem PC aus online die Bearbeitung von Urlaubs- und Fortbildungsanträgen und die Pflege von persönlichen Daten („Visitenkarte“: Name, Anschriften etc.) rollendefiniert ermöglicht werden soll.

Mit dem Finanzsenator ist vereinbart worden, dass es den Beschäftigten freigestellt bleiben muss, ob sie auf ihre Visitenkarte weitere Daten neben Namen und dienstliche Erreichbarkeit aufnehmen wollen. Auch sollen sie nicht verpflichtet werden, Anträge mit sensiblen Inhalten (z. B. Sonderurlaub zur Betreuung eines pflegebedürftigen Angehörigen) online zu beantragen.

Ich habe angeregt, eine Dreiteilung der Gesamtapplikation (Fortbildungsdatenbank, MiP-Datenbank und PuMa-Online-Datenbank) vorzunehmen. Dadurch würde ein administrativer Vollzugriff auf das Gesamtsystem verhindert. Der Senator für Finanzen hat bestätigt, diese Aufteilung vorzunehmen. Mit weiteren technischen und organisatorischen Maßnahmen soll gewährleistet werden, dass Beschäftigte jeweils nur auf die eigenen Daten zugreifen.

Auf der Netzwerk- und Transportebene sind durch den Einsatz von Firewalltechnologie und die Verwendung von als sicher angesehenen Protokollen (SSH, SSL) technische Datenschutzmaßnahmen vorgesehen, die bei entsprechender Installation einen angemessenen Schutz auf diesen Ebenen gewährleisten können.

5.2 Ein Leserbrief mit Folgen

In der Nordsee-Zeitung erschien ein Artikel, in dem ein Bürger seinem Unmut Luft machte. Ihm seien aus seinem Haus Gegenstände im Wert von ca. 10.000 Euro entwendet worden, er habe daraufhin bei der Polizei Anzeige erstattet und die vermutlichen Täter genannt. Erst nach zweieinhalb Monaten habe ihm die Kriminalpolizei mitgeteilt, nunmehr liege ein Durchsuchungsbeschluss vor. Die polizeiliche Aktion sei zum Scheitern verurteilt gewesen, denn so lange werde kein Diebesgut aufbewahrt. Der Leserbrief schloss damit, dass der Verfasser nach diesen Erfahrungen das Vertrauen in „unsere Polizei und die Rechtsstaatlichkeit" verloren habe. Wie es sich gehört, wurde der Leserbrief mit Namen des Leserbriefschreibers (unter Angabe des Stadtteils) veröffentlicht.

Dieser Leserbrief hatte Folgen, denn was sich aus der Zeitung nicht erkennen ließ: Der Leserbriefschreiber war Beschäftigter des Magistrats. Es dauerte nicht lange und mir lag eine Beschwerde des Leserbriefschreibers vor. Darin beklagte er, der Leiter der Ortspolizeibehörde Bremerhaven habe eben diesen Leserbrief zum Anlass genommen und ihm ein Antwortschreiben auf dem Dienstweg zukommen lassen. In diesem Brief seien u. a. nähere Angaben zu der Tat sowie zu seinen persönlichen Umständen enthalten. Durch die Übersendung dieses Briefes - offen auf dem Dienstwege - sei der Inhalt auch anderen Kollegen und Vorgesetzten zur Kenntnis gelangt. Er fühle sich dadurch in Misskredit gebracht und sehe darin einen Verstoß gegen Bestimmungen des Bremischen Datenschutzgesetzes (BremDSG).

Ich habe mich daraufhin an den Magistrat gewandt und unter Hinweis darauf, dass für den offenen Versand von Informationen aus Strafermittlungsakten keine Befugnis nach der Strafprozessordnung bestehe, um Auskunft gebeten. Dabei habe ich darauf aufmerksam gemacht, dass verantwortliche Stelle die Staatsanwaltschaft sei, die unter Beachtung der Vorschriften über den Datenschutz (z. B. Nr. 4 i.V.m. Nr. 15 und 16 der MiStra) zu entscheiden habe, ob und gegebenenfalls welche personenbezogenen Daten an einen Dienstvorgesetzten übermittelt werden sollen. Der Magistrat hat mir über den Leiter der Ortspolizeibehörde eine Stellungnahme zukommen lassen, in der hervorgehoben wurde, dass die Einbindung des Vorgesetzten bewusst geschehen sei, weil in dem Verhalten des Leserbriefschreibers als Angehöriger der Verwaltung ein bemerkens- und überprüfungswerter Umstand gesehen werde.

Da in der Sache parallel noch andere dienstrechtliche Maßnahmen angestrebt wurden, wollte ich dem Ausgang dieser Verfahren nicht vorgreifen. Gleichwohl habe ich Bedenken geäußert, ob in diesem Fall nicht die Meinungsfreiheit nach Art. 5 Abs. 1 Grundgesetz Vorrang vor der dienst– beziehungsweise arbeitsrechtlichen Loyalitätspflicht des Beschäftigten gehabt hätte und deshalb eine Einschaltung des Dienstvorgesetzten nicht erforderlich gewesen wäre. In jedem Falle aber hätte es ausgereicht und wäre auch nach dem BremDSG angemessen gewesen, wenn der Vorgesetzte unmittelbar in einem verschlossenen Briefumschlag über diesen Leserbrief informiert worden wäre.

Ich habe den Vorgang dann nicht weiter verfolgt, mich insbesondere nicht nach dem Ausgang der dienstrechtlichen Verfahren erkundigt, weil der Magistrat mir mitgeteilt hat, dass nunmehr „durch

interne Abstimmung sichergestellt sei, dass künftig Derartiges ausgeschlossen sei und der Vorgang somit ein Einzelfall bleibe“.

5.3 Alternierende Telearbeit

Seit mehreren Jahren betreibt der Senator für Finanzen die Einführung der Alternierenden Telearbeit in der bremischen Verwaltung. Alternierende Telearbeit bedeutet, dass die Mitarbeiter überwiegend von zu Hause aus online, aber mindestens zwei Werktage in der Woche in der Dienststelle arbeiten sollen. Hierüber habe ich zuletzt unter Ziff. 5.5 meines 22. Jahresberichts vom 31. März 2000 berichtet.

Datenschutzkonforme elektronische Datenübertragung: Bei der Teilnahme am Modellversuch wird die Verbindung des häuslichen Arbeitsplatzes mit dem bremischen Verwaltungsnetz (BVN) hergestellt. Da diese Verbindung über das Internet hergestellt wird, sind besondere technische Sicherheitsvorkehrungen zu treffen. Die Authentifizierung und Anschlusserkennung der Telearbeiter erfolgt über ein X.509-Zertifikat. Mit dessen Hilfe wird auch der gesamte Datenverkehr über das Internet mittels IPSEC verschlüsselt. Die Authentisierung des Telearbeiters gegenüber den Servern wird zusätzlich - wie bisher - über Nutzerkennung und Passwort durchgeführt. Für den Zugriff von außen wird nur ein zentrales dienstliches Postfach auf dem Mail-Server bei der Bremer Kommunikationstechnik (BreKom - Eigenbetrieb der Stadtgemeinde Bremen) freigegeben. Bei dieser Lösung haben die so verbundenen Teilnehmer keinen direkten Zugriff auf ihre zu bearbeitenden Daten in der Dienststelle. Alternativ erfolgt die direkte Durchschaltung durch das LAN der Dienststelle, aber dort nur bis zu einem Terminalserver. Terminalserver ermöglichen den visuellen Zugriff auf Client-Server-Verfahren bzw. Dokumente, ohne direkt auf die Verfahren bzw. Dokumente zugreifen zu müssen.

Abschluss des Modellversuchs: Nach Abschluss des Modellversuchs habe ich vorgeschlagen, die Verarbeitung sensibler personenbezogener Daten am häuslichen Arbeitsplatz nur dann zu erlauben, wenn es regelmäßig nicht ausreicht, diese während der Arbeitszeiten am dienstlichen Arbeitsplatz zu erledigen. Für diesen Fall soll neben dem regulär zu beteiligenden behördlichen Datenschutzbeauftagten meine vorherige Beteiligung sichergestellt werden. Außerdem bedarf es besonderer technischer Anforderungen am häuslichen Arbeitsplatz, z. B. ein verschließbares Arbeitszimmer. Ich werde den Fortgang der Alternierenden Telearbeit weiter beobachten.

6. Inneres

6.1 Prüfung von Polizeirevieren

In diesem Jahr habe ich datenschutzrechtliche Prüfungen von Polizeirevieren vorgenommen. Dabei habe ich folgende Mängel festgestellt:

- Die Zutrittskontrolle war teilweise nicht gewährleistet, da Serverräume und Datenschränke unverschlossen waren. In einem Fall war am Serverraum ein Hinweisschild „Tür nicht schließen“. Eine weitere Überprüfung durch den behördlichen Datenschutzbeauftragten der Polizei Bremen ist erforderlich.

- Bei der Begehung der Räumlichkeiten habe ich festgestellt, dass PC-Arbeitsplätze trotz Abwesenheit der Bediensteten nicht gegen unbefugte Nutzung und unbefugte Einsichtnahme gesperrt waren. Neben einem ausdrücklichen Hinweis an die Mitarbeiter, die Arbeitsplätze bei Verlassen der Räume zu sichern, empfehle ich hier, die Konfiguration der PCs so vorzunehmen, dass sie nach einer bestimmten Zeit der Nichtnutzung automatisch gesperrt werden. Aus datenschutzrechtlicher Sicht wird weiterhin der Einsatz von Chipkarten mit Kennwort seit Jahren von mir gefordert.

- Der ordnungsgemäße Umgang mit Datensicherungsbändern war nicht gegeben. Während in einem Fall die Bänder in offenen Regalen gelagert wurden, waren in einem anderen Fall Datenbänder mit unbekannter Herkunft und unbekanntem Inhalt im Serverraum vorhanden. Hier ist eine entsprechende Anweisung gegenüber den Verantwortlichen der einzelnen Reviere zu erteilen, um die Mitarbeiter zu sensibilisieren und den ordnungsgemäßen Umgang mit Datensicherungsmedien zu gewährleisten.

- An den Internet-Arbeitsplätzen wurden USB-Anschlüsse (Universal Serial Bus) für die Übernahme von Bilddaten dienstlicher Kameras zur Nutzung freigegeben. Die Freischaltung von USB-Anschlüssen stellt grundsätzlich ein Risiko dar. Über diese Schnittstelle lassen sich diverse Hardwarekomponenten wie z. B. CD-ROM-Laufwerke und Festspeicher-Medien anschließen. Es müssen daher Maßnahmen ergriffen werden, um den Zugriff über einen USB-Anschluss auf die zur Nutzung der definierten und zugelassenen Komponenten zu beschränken. Selbst aber bei Beschränkung der Nutzung auf Speichermedien für digitale Kameras besteht dennoch die Möglichkeit, nicht nur Bilddateien, sondern auch Dateien in anderen Formaten (z. B. Worddateien, ausführbare Programme) in das Netz und aus dem Netz heraus zu transferieren. Hier liegt potentiell eine Gefährdung durch Umgehung der Weitergabekontrolle vor. Zwar wurde mir versichert, mit einer speziellen Software dafür zu sorgen, dass eine Prüfung der zu transferierenden Dateien und genutzten Endgeräte stattfindet, es liegt derzeit allerdings kein Datenschutzkonzept vor, das den Einsatz von USB-Anschlüssen grundsätzlich und den Anschluss digitaler Kameras im Speziellen regelt.

- Für die Internetnutzung steht in den geprüften Revieren ein Standalone-PC zur Nutzung zur Verfügung. Obwohl kein ausreichender Schutz auf diesen Rechnern installiert war, waren dienstliche und personenbezogene Daten auf diesen PCs zu finden, darunter Schichtpläne und auch dienstliche Bilddateien, die wiederum über einen vorhandenen USB-Anschluss auf den

Rechner gelangt waren. Darüber hinaus war an diesen Rechnern teilweise eine Anmeldung ohne Passwort möglich. Da die Administration dieser Rechner durch die Bediensteten ebenfalls möglich war, konnte durch die Verantwortlichen keine verbindliche Aussage darüber gemacht werden, welche Software auf dem Rechner vorhanden ist und welcher Mitarbeiter welche Dateien auf diesen Rechner kopiert und bearbeitet hat. Es ist nicht zulässig, auf einem PC-Arbeitsplatz, der ausschließlich für die Internetnutzung eingerichtet worden ist und der darüber hinaus neben einem Virenschutz keinen besonderen Sicherheitsmaßnahmen unterliegt, personenbezogene Daten zu speichern. Für mich sind weiterhin keine Gründe erkennbar, wieso Bedienstete über die Möglichkeit verfügen müssen, die Rechner zu administrieren. Ein entsprechendes Datenschutzkonzept, das den Einsatz von Rechnern mit Internetanschlüssen in den Revieren regelt, ist erforderlich.

- Problematisch ist außerdem die Anmeldung der Polizeibeamten am so genannten Arbeitsplatz „Wache“. Beamte, die kurzfristig den Arbeitsplatz verlassen, melden sich nicht am PC ab. Wenn in dieser Zeit andere Kollegen die Funktion des Arbeitsplatzes übernehmen, werden Abfragen und Arbeiten unter der Benutzerkennung des abwesenden Mitarbeiters vorgenommen. Somit ist eine Eingabekontrolle nicht mehr gewährleistet. Unter Gewährleistung der Praktikabilität ist hier eine Lösung zu erarbeiten. In den geprüften Revieren waren keine Chipkarten zur Anmeldung im Einsatz.
- Für das in den Revieren eingesetzte Softwareprodukt RevierS lag zum Zeitpunkt der Prüfung keine Verfahrensbeschreibung vor. Es handelt sich um ein datenbankbasiertes Programm, welches Unterstützung in den Bereichen Personalplanung, Personalverwaltung, Stundenabrechnung, Personalsteuerung sowie Kosten- und Leistungsrechnung bietet und in diesen Bereichen zahlreiche Funktionen zur Verfügung stellt. In dieses Produkt integriert ist die Dokumentation von Tätigkeiten während des Dienstes und die Führung des Wachbuchs.

Auf die Problematik eines so genannten öffentlichen Laufwerks, für das kein Datenschutzkonzept vorlag, gehe ich im nachfolgenden Punkt näher ein.

Meinen Prüfungsbericht habe ich dem behördlichen Datenschutzbeauftragten der Polizei Bremen übergeben; er nahm inzwischen Stellung. Er teilte mit, dass es beabsichtigt ist, durch Aktivierung eines Bildschirmschoners mit Passwortschutz eine unberechtigte Nutzung zu verhindern. Darüber hinaus sollen die Mitarbeiter verstärkt sensibilisiert und auf ihre Verpflichtung hingewiesen werden, die Dienstzimmer bei Abwesenheit zu verschließen.

Zur Sicherung der Serverräume und Datensicherungen gab er an, dass durch weitere organisatorische Maßnahmen und Kontrollen zukünftig die konsequente Einhaltung der Vorgaben der Richtlinien für die IT-Sicherheit der Polizei in Bremen erreicht werden solle, welche die Notwendigkeit einer ausreichenden Sicherung von Servern, Serverräumen, Schränken und Datenträgern vorsehen. Fehlende Schränke zur Verwahrung der Datensicherungsmedien würden bereitgestellt.

Der Datenschutzbeauftragte der Polizei Bremen teilte weiterhin mit, dass eine Neukonfiguration der Internet-Rechner stattfinden werde. Die Polizei hält jedoch eine einzelfallbezogene Vergabe von

Administrationsrechten für erforderlich. Gründe für die Forderung wurden nicht genannt und müssen daher noch weiter abgeklärt werden.

Ferner erklärte der Datenschutzbeauftragte der Polizei, dass die technische Infrastruktur für ein Anmeldeverfahren per Chipkarte weitestgehend geschaffen und eine Umstellung der Polizeiwachen erfolgt sei. Die Chipkarten seien bei Verlassen des Arbeitsplatzes aus dem Kartenlesegerät zu entfernen.

Die Verfahrensbeschreibung für das Softwareprodukt RevierS wurde durch die Polizei Bremerhaven eingereicht und befindet sich in der Prüfung. Für die Polizei Bremen steht die Verfahrensbeschreibung noch aus.

Ich erwarte nun noch ein Datenschutzkonzept, das den Einsatz von USB-Anschlüssen im Allgemeinen und den Anschluss dienstlicher Kameras im Speziellen regelt.

6.2 Alte Gewohnheiten und moderne DV bei der Polizei

Im Rahmen der datenschutzrechtlichen Prüfungen habe ich unter anderem untersucht, wie die Nutzung von zentralen Laufwerken zur Ablage von Textdateien geregelt ist. Neben der Möglichkeit, Dateien zum ausschließlich eigenen Gebrauch in einem persönlichen Laufwerk abzulegen sowie Dateien für bestimmte Mitarbeitergruppen bereitzustellen, wurde die Nutzung eines so genannten öffentlichen Laufwerks technisch zur Verfügung gestellt. Hierbei handelt es sich um einen Festplattenbereich, in dem ursprünglich nur größere Dateien zum Austausch zwischen zwei Mitarbeitern bereitgestellt und nach der Übergabe wieder gelöscht werden sollten. Auf diesen Bereich haben grundsätzlich alle Bediensteten der Polizei Zugriff.

Während der Prüfung konnten vor Ort von den Bediensteten keine Angaben über den weiteren Umgang mit diesen Daten gemacht werden, da das Laufwerk zentral verwaltet wird. Später wurde dargelegt, dass dieser Speicherbereich zwischenzeitlich nicht mehr nur dem alleinigen Austausch von Daten diene, sondern auch organisationsübergreifend zur täglichen Ermittlungsarbeit genutzt werde. Eine regelmäßige Löschung dieses Plattenbereichs wurde nicht durchgeführt. So verblieb eine Vielzahl von Dateien auf dem Plattenbereich. Eine Regelung zur Löschung der dort gespeicherten Daten gab es nicht. Ich forderte daher in meinem Prüfbericht die Auflösung dieses Laufwerks in seiner bestehenden Form.

Der Datenschutzbeauftragte der Polizei folgte meiner Auffassung und die Polizei Bremen hat zwischenzeitlich die Auflösung dieses Laufwerks vollzogen. In seiner schriftlichen Stellungnahme teilte der Datenschutzbeauftragte mit, dass ein zusätzliches Laufwerk angelegt worden ist, in dem Dateiordner für geschlossene Benutzergruppen eingerichtet werden, wobei die Zugriffsberechtigungen den dienstlichen Erfordernissen entsprechend definiert werden.

Das bestehende öffentliche Laufwerk wurde gelöscht und steht dem ausschließlichen kurzfristigen Datenaustausch nur noch insoweit zur Verfügung, als sich die Daten nicht über E-Mail oder bereits bestehende Verzeichnisse übertragen lassen. Der behördliche Datenschutzbeauftragte der Polizei sicherte zu, dass das öffentliche Laufwerk wöchentlich komplett gelöscht wird.

6.3 DNA-Reihenuntersuchung in Bremerhaven

Erst aus der Presse habe ich erfahren, dass die Ortspolizeibehörde Bremerhaven zur Aufklärung verschiedener Straftaten gegen Frauen für Mitte Mai 2004 eine DNA-Reihenuntersuchung von über 2.000 Männern geplant hatte. Auslöser der Presseveröffentlichung war, dass die geplante DNA-Reihenuntersuchung von der Generalstaatsanwältin gestoppt worden war. Sie war der Auffassung, dass für die DNA-Reihenuntersuchung auf freiwilliger Basis ein richterlicher Beschluss erforderlich sei. Ich teile diese Auffassung.

Die Untersuchung der DNA stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Nur durch einen Richterbeschluss sind verfahrensrechtliche Vorgaben sichergestellt. Ich schaltete mich ein und bat die Ortspolizeibehörde Bremerhaven, mir zur datenschutzrechtlichen Bewertung die Entwürfe des Einladungsschreibens und der Einwilligungserklärung sowie Aufklärungsmaterial zu übersenden. Bei dem mir übersandten Einladungsschreiben fiel sofort auf, dass die Einladung zur freiwilligen Abgabe einer Speichelprobe als „Vorladung“ gekennzeichnet war. Sie war zudem in der Diktion so gehalten, dass die „Freiwilligkeit der Abgabe der Speichelprobe“ nicht hinreichend deutlich wurde. In mehreren Diskussionsrunden mit der Ortspolizeibehörde Bremerhaven wurden die Unterlagen neu gestaltet. Außerdem wies ich in den Gesprächen auf folgende datenschutzrechtliche Anforderungen hin:

- Aufklärung des betroffenen Personenkreises über seine Rechte.
- Eng eingegrenzte Untersuchungskreise (Alter, Stadtteile). Eine Ausweitung auf den nächst größeren Kreis darf nur dann erfolgen, wenn die Maßnahme im engeren Kreis erfolglos geblieben ist.
- Es ist sicherzustellen, dass nur erforderliche Daten erhoben werden.
- Die Daten (Spuren, Probedaten, usw.) sind frühestmöglich zu löschen.
- Es ist zu verhindern, dass die Daten für andere Zwecke verwendet werden. Das heißt, nur Abgleich mit dem Spurenmaterial, kein Abgleich mit der DNA-Datei beim BKA.

Am 20. April 2004 erging die für eine DNA-Reihenuntersuchung erforderliche richterliche Anordnung, so dass mit der Durchführung begonnen werden konnte.

Während der laufenden Untersuchung führte ich eine Zwischenkontrolle durch, um mich zu vergewissern, dass die o. g. datenschutzrechtlichen Anforderungen hinreichend Berücksichtigung finden.

Ich erhielt im Rahmen dieser Überprüfung folgende Informationen: Zur Abgabe der Speichelprobe waren ca. 2.300 Männer aufgerufen, die in einem bestimmten Bremerhavener Stadtgebiet wohnen bzw. gewohnt haben. An der Speichelprobe haben bis zum Oktober 2004 ca. 92 % der in Frage kommenden Personen teilgenommen. Die Speichelproben wurden im ersten Durchgang nur auf drei von acht Merkmalen untersucht und mit den Tatortspuren verglichen. Bisher wurde keine Übereinstimmung durch die beauftragte Untersuchungsstelle beim LKA Bremen festgestellt. Die

Proben wurden nach der Auswertung laufend vernichtet. Probleme bereitet der Polizei in Bremerhaven die Weigerung von ca. 80 bis 100 Personen, die trotz mehrmaliger Ansprache nicht zur Abgabe einer Speichelprobe bereit waren. Da es sich um einen Aufruf zur freiwilligen Abgabe der DNA handelt, kann selbstverständlich jeder Bürger von dem Recht der Verweigerung Gebrauch machen. Der Polizei bleibt nur die Möglichkeit, auf der Basis der Strafprozessordnung in den Fällen weiter zu ermitteln.

Über den Verlauf der DNA-Reihenuntersuchung in Bremerhaven habe ich in drei Sitzungen dem Rechtsausschuss der Bremischen Bürgerschaft berichtet. Da es keine ausdrückliche Rechtsgrundlage für DNA-Reihenuntersuchungen in der Strafprozessordnung gibt, habe ich darüber hinaus die Schaffung einer solchen gesetzlichen Grundlage mit präzisen und engen Anforderungen gefordert. Hierdurch würde Rechtssicherheit für alle am Verfahren Beteiligten geschaffen werden.

6.4 Videoüberwachung auf dem Bahnhofsvorplatz

Durch die Änderung des Bremischen Polizeigesetzes (BremPolG, § 29 Abs. 3) im Jahr 2001 wurde die Befugnis geschaffen, dass die Polizei öffentliche Orte, an denen vermehrt Straftaten begangen werden oder bei denen aufgrund der örtlichen Verhältnisse die Begehung von Straftaten besonders zu erwarten ist, durch Videoanlagen überwachen darf. Von dieser Regelung hat die Polizei Bremen im Jahre 2002 Gebrauch gemacht. Mit Zustimmung des Senators für Inneres und Sport hat der Polizeipräsident eine entsprechende Anordnung für die Videoüberwachung des Bahnhofsvorplatzes erlassen und am 4. Oktober 2002 eine Videokamera auf dem Bahnhofsvorplatz und die erforderlichen Beobachtungs- und Aufzeichnungseinrichtungen im Einsatz- und Lagezentrum des Polizeipräsidiums in Betrieb genommen (zu den dabei anstehenden Fragen vgl. 25. JB, Ziff. 6.1 und 26. JB, Ziff. 4.2).

Im Laufe des Berichtsjahres wurde die Beobachtungs- und Aufzeichnungstechnik vom Polizeipräsidium in die Wache „Stephanitor“ verlegt, weil sich die schwerpunktmäßige Einsatzbildung und die Informationsgewinnung durch die Beobachtung des Geschehens auf dem Bahnhofsvorplatz an verschiedenen Orten als nicht sinnvoll herausgestellt hat. Über diese Änderung wurde ich zwar unterrichtet, aber mir liegt noch keine Neufassung der oben genannten Anordnung oder ein Datenschutzkonzept vor.

§ 29 Abs. 3 BremPolG schreibt vor, dass in regelmäßigen Abständen zu prüfen ist, ob die Voraussetzungen für die Videoüberwachungsanordnung noch bestehen. In der Anordnung wurde bestimmt, dass eine Überprüfung in zweijährigen Abständen zu erfolgen hat. Daraufhin hat zum 3. November 2002 der Senator für Inneres und Sport der Deputation für Inneres einen entsprechenden Bericht vorgelegt. Darin kommt der Senator für Inneres und Sport zu einem positiven Ergebnis und verlangt, wie ich der Presse entnehmen konnte, eine Ausweitung der Videoüberwachung durch die Polizei auch auf andere Standorte (Sielwall, Vegesack, u. a.). Diesem positiven Ergebnis ist in der politischen Diskussion widersprochen worden. So wurde auf veränderte Rahmenbedingungen (Abbau der Fahrradständer und Einrichtung einer bewachten Fahrradgarage) oder auf die Verdrängung der Drogenszene von dem Bahnhofsvorplatz auf einen Park hinter dem Bahnhof verwiesen.

Auf besondere Anforderung habe auch ich den oben genannten Bericht erhalten. Bevor eine vorschnelle Ausweitung der Videoüberwachung auf andere Bereiche erfolgt, sollten zuvor die Ergebnisse ausführlich untersucht und bewertet werden.

6.5 Automatisiertes Fingerabdruck-System - AFIS

Die von der Ortspolizeibehörde Bremerhaven eingesetzte Anwendung dient der Verwaltung und Verarbeitung der im Rahmen der erkennungsdienstlichen Behandlung erhobenen Finger- und Handflächenabdrücke und der an Tatorten gefundenen Finger- und Handflächenabdrücke vorwiegend nach § 81b Strafprozessordnung (StPO) und § 11a Bremisches Polizeigesetz (BremPolG). Die Daten werden in einer kleinen vernetzten Oracle-Datenbank verwaltet, auf die nur die Mitarbeiter der Organisationseinheit „Erkennungsdienst“ (ED) Zugriff haben.

Die Datei hat den Zweck, die Identifizierung von bisher unbekannten Spurenverursachern und von Personen, die bereits im ED-Bestand sind, zu erleichtern.

Von der erkennungsdienstlichen Behandlung können betroffen sein:

- Beschuldigte,
- Tatverdächtige,
- Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie künftig Straftaten begehen werden.

Die Finger- und Handflächenabdrücke werden eingescannt und zusammen mit dem Namen, dem Vornamen und der Lichtbildnummer in die AFIS-Datei eingespeichert, soweit die rechtlichen Voraussetzungen für eine erkennungsdienstliche Behandlung vorliegen.

Die gespeicherten Daten werden auf Grundlage des § 489 StPO bzw. analog zu den Richtlinien für die Aufbewahrung kriminalpolizeilicher personenbezogener Sammlungen (KPS-Richtlinien) gelöscht.

Bei einem Treffer im AFIS-System wird anhand der Originalabdrücke ein herkömmliches daktyloskopisches Gutachten erstellt.

Ich habe der Ortspolizeibehörde empfohlen, für die Speicherung, den Zugriff und die Löschung der Daten im AFIS die Protokollierung so zu gestalten, dass die Nutzung des Systems jederzeit nachvollziehbar ist. Vor einem evtl. zukünftigen Betrieb von AFIS im zentralen Netzwerk der Ortspolizeibehörde sind die Administrationsrechte neu zu gestalten.

6.6 Prüfung der Telekommunikationsüberwachung

Mir wurden vom Senator für Inneres und Sport der Entwurf der „Richtlinien für das taktische Vorgehen anlässlich einer Telekommunikationsüberwachung (TKÜ) gemäß §§ 100 a ff Strafprozessordnung (StPO)" und der Entwurf der „Errichtungsanordnung der Arbeitsdatei PAT“ (Programm zur Auswertung von Telekommunikationsüberwachungen) übersandt. Da die Errichtungsanordnung einige technische und organisatorische Fragen offen ließ, kam es zu einem Gespräch mit den zuständigen Administratoren und dem behördlichen Datenschutzbeauftragten der Polizei Bremen. Hierbei wurde deutlich, dass es sich bei der Arbeitsdatei PAT um ein DV-Programm handelt, welches zur Aufnahme der Verbindungsdaten (z. B. Rufnummern der Teilnehmer, Datum und Uhrzeit des Gesprächs) und der Verschriftung der abgehörten Gesprächsinhalte dient. Der Arbeitsdatei vorgeschaltet ist ein Aufzeichnungssystem, das automatisch die Gesprächs- und Verbindungsdaten speichert. Datenschutzrechtlich bedeutsam sind Fragen insbesondere der Nutzung, des Zugangs, der Datensicherung und der Löschung der aufgezeichneten Telekommunikationsdaten.

Die bestehende Errichtungsanordnung reicht nicht aus, um den Ablauf der Telekommunikationsüberwachung zu beschreiben. Ich halte es für erforderlich, zur Beschreibung des Gesamtverfahrens die bestehende Verfahrensbeschreibung um die Erläuterung der technischen und organisatorischen Maßnahmen des vorgeschalteten Systems, welches technisch zur Aufnahme der Gespräche dient, zu ergänzen. Des Weiteren stellte ich fest, dass die Errichtungsanordnung weder dem gegenwärtigen Stand entspricht noch konsequent umgesetzt worden ist. Ich fordere daher eine entsprechende Aktualisierung und Umsetzung. Neben der Arbeitsdatei PAT sind darüber hinaus weitere Verschriftungsprogramme im Einsatz, die nicht dokumentiert sind und für die ich ein Einsatzkonzept fordere. In diesem Zusammenhang traten weiterhin Fragen zur Zugangsregelung und dem Einsatz von USB-Anschlüssen auf, die bisher nicht geklärt werden konnten. Mein Bericht wurde dem Datenschutzbeauftragen der Polizei Bremen übergeben, seine Antwort steht noch aus.

6.7 ISA-Web statt NIVADIS

Im Jahr 2003 war man noch zuversichtlich, im Laufe dieses Berichtsjahres das von Niedersachsen entwickelte Vorgangsbearbeitungssystem NIVADIS einzuführen. Im Sommer 2004 wurde davon Abstand genommen. Ursachen waren u. a. technische und finanzielle Gründe.

Mit der Entscheidung einher ging der Auftrag, das von der Polizei im Land Bremen verwendete Verfahren ISA (Informationssystem Sachen und Anzeigen) weiter zu entwickeln und webbasiert umzugestalten.

Ich habe den Senator für Inneres und Sport sowie die Polizei darauf hingewiesen, dass die bei der Planung für die Vorgangsbearbeitungssysteme EVA-HB und NIVADIS entwickelten datenschutzrechtlichen Standards auch für die Umgestaltung von ISA nach ISA-Web gelten.

Zu den datenschutzrechtlichen Rahmenbedingungen gehören u. a.

- die Nachvollziehbarkeit der Zulässigkeit der Erhebung und Speicherung von Daten,
- die Gewährleistung der Zweckbindung der weiteren Datenverarbeitung, insbesondere bei der Datenübermittlung, -veränderung oder -nutzung,
- die revisionssichere Protokollierung der Datenverarbeitung im System (z. B. Kenntnisnahme, Auswertung, Veränderung oder Löschung),
- die Gewährleistung des Auskunfts- und Akteneinsichtsrechts,
- die Sicherstellung der Eindeutigkeit der Person des Betroffenen, um Verwechselungen auszuschließen und
- dass gewährleistet wird, dass Daten, die mit besonderen Mitteln und Methoden (z. B. Observation) erhoben wurden, extra gekennzeichnet werden.

Anfang Januar 2005 wurde mir ein erster Prototyp von ISA-Web vorgestellt, an dem aber noch nicht die vorstehenden Rahmenanforderungen geprüft werden konnten.

6.8 Sicherheitsmaßnahmen bei Verlust der Kredit- oder EC-Karte

Die Ortspolizeibehörde Bremerhaven hat ein auch von der Polizei Bremen übernommenes Verfahren entwickelt, mittels dessen die Angaben zu Debit- und Kreditkarten erfasst werden, die durch Diebstahl oder Verlust abhanden gekommen sind oder betrügerisch / missbräuchlich genutzt werden.

Die Angaben der Debit- und Kreditkarten (Bankleitzahl, Kontonummer und ggf. Kartenfolgenummer bzw. Kreditkartennummer) werden bei dem anzeigenden Bürger von der Polizei aufgenommen, geprüft und dann an Unternehmen weitergeleitet, die dem „KUNO“-Sperrsystem beigetreten sind. Die Unternehmen veranlassen daraufhin die Sperrung des entsprechenden Kontos (für maximal 10 Tage) bzw. der abhanden gekommenen Debit- und Kreditkarte, soweit eine Kartenfolgenummer bekannt ist.

Bei der Polizei werden darüber hinaus Familienname, Vorname, Postleitzahl, Wohnort, Straße, Hausnummer und Telefonnummer der betroffenen Person gespeichert. Alle Angehörigen der Vollzugspolizei sind berechtigt, Daten in dieses System einzugeben.

Abfragen können dieses System aber nur die Mitarbeiter der Kriminalpolizei, die mit der Bearbeitung von verlorenen oder entwendeten Kreditkarten befasst sind.

Gegen das Verfahren „KUNO“ werden aus datenschutzrechtlicher Sicht keine Bedenken erhoben.

6.9 Arbeitsentwurf zur Änderung des Bremischen Polizeigesetzes

Im März 2004 übersandte mir der Senator für Inneres und Sport den Entwurf zur Änderung des Bremischen Polizeigesetzes (BremPolG). Dieser Entwurf lehnt sich fast vollständig an das Niedersächsische Polizeigesetz an, weil vorgesehen war, das Datenverarbeitungsprogramm NIVADIS, das in Niedersachsen eingesetzt wird, auch in Bremen zu übernehmen.

Ich habe zu dem Entwurf eine Stellungnahme abgegeben und insbesondere zu folgenden Regelungen datenschutzrechtliche Bedenken erhoben:

Überwachung der Telekommunikation durch die Polizei: Der Entwurf sieht eine weitgehende Überwachung der Telekommunikation zur Gefahrenabwehr und zur vorbeugenden Strafverfolgung vor. Gegen diese Erweiterung polizeilicher Befugnisse habe ich unter Hinweis auf die Entscheidungen des Bundesverfassungsgerichts zum Lauschangriff (vgl. Ziff. 7.1 dieses Berichts) und das anhängige Verfahren vor dem Bundesverfassungsgericht zur Telekommunikationsüberwachung nach § 33 a des Niedersächsischen Polizeigesetzes datenschutzrechtliche Bedenken erhoben. Der Senator für Inneres und Sport hat bereits signalisiert, den Entwurf zu überarbeiten.

Identitätskontrollen, Durchsuchung und erkennungsdienstliche Behandlung: Der Entwurf sieht eine Identitätskontrolle einschließlich einer Durchsuchung und/oder erkennungsdienstlichen Behandlung von Personen vor, die sich an einem Ort befinden, an dem Straftaten von erheblicher Bedeutung verabredet werden oder sich Straftäter verbergen. Gegen diese Möglichkeit zur Einschränkung der unkontrollierten Bewegung im öffentlichen Raum habe ich Bedenken erhoben, weil bereits die zufällige Anwesenheit und nicht das „Aufhalten“ einer Person umfassende polizeiliche Maßnahmen nach sich ziehen kann.

Einrichtung von Kontrollstellen: § 11 a des Gesetzentwurfs sieht die Einrichtung von Kontrollstellen vor. Danach dürfen Kontrollstellen auch auf öffentlichen Plätzen und Straßen eingerichtet werden, wenn bestimmte Straftaten begangen werden sollen und diese durch die Kontrollstellen verhütet werden können.

Der Straftatenkatalog ist zu weit gefasst und eine Speicherung der daraus gewonnenen Daten soll auf Vorrat möglich sein, ohne dass der Betroffene davon Kenntnis erlangen kann.

Taschenkontrollen und Befragungsrecht bzw. Auskunftspflicht: Der Entwurf sieht die Befugnis der Polizei zur Vorsorge für die Verfolgung von Straftaten mit internationalem Bezug vor, dass Bürger praktisch jederzeit befragt und um Auskunft gebeten und dass mitgeführte Sachen eingesehen werden können. Ein solcher Eingriff in das Persönlichkeitsrecht wäre unverhältnismäßig. Dies gilt insbesondere auch für die „Inaugenscheinnahme mitgeführter Sachen“. Hinsichtlich einer Befragung wäre dem Betroffenen zu eröffnen, wozu er sich äußern soll, dass er sich nicht selbst belasten muss und welchem Zweck die Befragung dient. Durch diese Vorschrift („internationaler Bezug“) wären naturgemäß insbesondere ausländische Mitbürger betroffen.

Speicherung in Akten zur Sicherung in Dateien: § 36 a BremPolG schreibt vor, dass Daten, die länger als sechs Monate gespeichert werden sollen, nur dann in elektronischen Dateien gespeichert werden

dürfen, wenn ihr Inhalt sich auch aus Akten erschließt. Der Entwurf sieht eine Aufhebung dieser Vorschrift vor.

Gegen die Streichung der Regelung habe ich datenschutzrechtliche Bedenken erhoben. Da noch nicht bekannt ist, ob ein neues Vorgangsbearbeitungssystem hinreichend revisionssicher ist und jederzeit nachvollzogen werden kann, wer welche Datenverarbeitung verantwortet, ist die Beibehaltung dieser Vorschrift, insbesondere unter Beachtung des § 7 Abs. 4 Nr. 5 Bremisches Datenschutzgesetz (BremDSG), geboten. Eine vollständige Streichung würde auch andere DV-Systeme, die die Polizei betreibt, von einer Belegpflicht entbinden.

Wohnraumüberwachung durch die Polizei: Die geltenden Vorschriften des § 33 BremPolG sehen die Möglichkeiten der Polizei zur Wohnraumüberwachung vor. Auf der Grundlage der vorgenannten Entscheidung des Bundesverfassungsgerichts vom 3. März 2004 ist auch diese neu zu gestalten.

6.10 Arbeitsentwurf eines Gesetzes über den Verfassungsschutz

Im Sommer des Berichtsjahres erhielt ich erneut einen Entwurf mit Änderungen zum Verfassungsschutzgesetz im Lande Bremen. Ich habe dazu eine Stellungnahme abgegeben und insbesondere zu folgenden Regelungen datenschutzrechtliche Bedenken erhoben:

- Wohnraumüberwachung

  Die Entscheidung des Bundesverfassungsgerichts zum Lauschangriff (vgl. Ziff. 7.1 dieses Berichts) war noch nicht berücksichtigt bei den Regelungen über das audio-visuelle Erheben und Aufzeichnen von Daten aus Wohnungen. Der Entwurf berücksichtigte insoweit weder materiellrechtliche noch verfahrensmäßige Vorkehrungen, die bei Eingriffen in den sog. Kernbereich privater Lebensgestaltung neben den technischen Sicherungsmaßnahmen vorzusehen sind.

- Schutz von Amts- und Berufsgeheimnisträgern

  Der Gesetzentwurf sah keine rechtlichen und verfahrenssichernden Maßnahmen vor, die den Schutz von Amts- und Berufsgeheimnisträgern (z. B. Verteidigern) entsprechend § 53 Strafprozessordnung (StPO) garantieren.

- Hilfeleistung bei der Verwendung von Tarnmitteln

  Der Entwurf sieht, wie auch die vorherigen, die Verpflichtung für öffentliche Stellen vor, dass sie bei der Bereitstellung von Tarnmitteln (Ausweisen, Legenden usw.) auch dann Unterstützung zu leisten haben, wenn ein Interessenkonflikt bestehen könnte. Ich habe dagegen Bedenken erhoben, denn dadurch kann die Aufgabenerfüllung der verpflichteten Behörde oder Stelle (etwa des Landesbeauftragten für den Datenschutz oder der Ausländerbeauftragten) ernsthaft gefährdet werden. Auch muss sichergestellt werden, dass dem Verfassungsschutz auf diese Weise weitergehende Rechte eingeräumt werden (z. B. polizeiliche Rechte), als ihm nach dem Landesverfassungsschutzgesetz zustehen. Ich habe dazu entsprechende Änderungen vorgeschlagen.

- Minderjährigenregelungen

  Der Entwurf sieht Regelungen vor, die Speicherung von Daten Minderjähriger bereits mit dem 14. Lebensjahr zu gestatten, während das nachrichtendienstliche Informationssystem (NADIS) eine solche Speicherung erst ab dem 16. Lebensjahr zulässt. Die Speichererlaubnis sollte sich auf Personen ab dem 16. Lebensjahr beschränken. Ich habe darüber hinaus weitergehende datenschutzrechtliche Sicherungen (Sperrung und frühzeitige Löschung) vorgeschlagen.

- Datenschutzrechtliche Bestimmungen im Entwurf

  Der Gesetzentwurf sieht eine Reihe von bereichsspezifischen datenschutzrechtlichen und archivrechtlichen Bestimmungen vor. Gegen eine Regelung im Verfassungsschutzgesetz habe ich Bedenken erhoben, da diese Materie im Bremischen Datenschutzgesetz und auch im Bremischen Archivgesetz ausreichend geregelt ist.

- Veröffentlichung von personenbezogenen Daten durch den Verfassungsschutz

Der Gesetzentwurf sieht für Zwecke der Öffentlichkeitsaufklärung die Veröffentlichung von personenbezogenen Daten durch den Verfassungsschutz vor. Ich habe vorgeschlagen, dass in jedem Fall vor der Veröffentlichung personenbezogener Daten zu prüfen ist, ob eine Benachrichtigung des Betroffenen geboten ist. Diese Regelung soll Betroffene vor Überraschungen schützen und sie in die Lage versetzen, auf Irrtümer und Fehler hinzuweisen.

6.11 Bürgerbüro Bremerhaven

Der Magistrat der Stadt Bremerhaven hat im Berichtsjahr im neu geschaffenen „Hanse-Carré“ der Seestadt das Bürgerbüro Bremerhaven eingerichtet. Ähnlich wie in dem von der Stadt Bremen eingerichteten Bürger-Service-Center (vgl. 26. JB, Ziff: 6.3.2) sollen dort dem Bürger unterschiedliche Dienstleistungen der Stadt angeboten werden. Die Dienstleistungen betreffen u. a. Melde- und Passangelegenheiten, Straßenverkehrs- sowie Staatsangehörigkeits- und Ausländerangelegenheiten der Bürger.

Auch mit der Einrichtung des Bürgerbüros Bremerhaven sind erhebliche datenschutzrechtliche Fragestellungen verbunden. Da die zu verarbeitenden personenbezogenen Daten häufig sehr sensibel sind, ist die Ergreifung angemessener technischer und organisatorischer Sicherungsmaßnahmen durch das Bürgerbüro von besonderer Bedeutung. Unter anderem habe ich eine klare räumliche Trennung des Empfangs- und des Abfertigungs- bzw. Servicebereichs und innerhalb des letztgenannten Bereichs eine schützende Abgrenzung der einzelnen Service-Einheiten untereinander empfohlen. Für die einzelnen Bereiche gelten datenschutzspezifische Anforderungen. So dürfen die Mitarbeiter des Bürgerbüros bei Staatsangehörigkeits- und Ausländerangelegenheiten Anträge zwar entgegennehmen, zur weiteren Bearbeitung müssen diese dann aber an das Fachamt weitergeleitet werden.

Vom Magistrat der Stadt Bremerhaven ist mir die Umsetzung der notwendigen Maßnahmen und die Einhaltung der zu beachtenden Anforderungen zugesagt worden. Ich werde die Einhaltung überprüfen.

6.12 Vollständige Ausländerakte an das Gesundheitsamt

Die Ausländerbehörde ersucht das Gesundheitsamt Bremen um Abgabe amtsärztlicher Gutachten zur Beurteilung, ob gemäß § 53 Ausländergesetz (AuslG) ein Abschiebehindernis besteht oder ob gemäß § 55 AuslG Duldungsgründe vorliegen. Mit dem Ersuchen wird u. a. um Auskunft gebeten, ob akute Erkrankungen bestehen, die der Reisefähigkeit entgegenstehen, wie lange die Behandlung dauert oder auch welche weiteren Behandlungsschritte erforderlich sind. Dazu wurde in der Vergangenheit die gesamte Ausländerakte dem Gesundheitsamt übersandt.

Gemäß § 13 Abs. 1 Bremisches Datenschutzgesetz (BremDSG) sind nur die Daten zu übermitteln, die zur rechtmäßigen Erfüllung der Aufgaben erforderlich sind, d. h., nur Daten, die der Ersuchte für seine Aufgabe benötigt. Dies können nur Daten sein, die die ärztliche Begutachtung unterstützen. In der Ausländerakte sind eine Vielzahl von Daten über den Betroffenen (Arbeitsverhältnisse, Strafverfahren, Fluchtdaten, Asylantragsdaten usw.), aber auch Daten über Dritte (Familienangehörige, Arbeitgeber, Zeugen, Vermieter u. v. a. m.) enthalten, die für eine amtsärztliche Begutachtung nicht erforderlich sind.

Das Gesundheitsamt hat in einem Anforderungsprofil die Informationen aufgeführt, die es für Gutachten zur Reisefähigkeit benötigt. Dies entspricht auch meinen Vorstellungen. Dieses Anforderungsprofil hat die Ausländerbehörde dem Senator für Inneres und Sport zur Entscheidung übergeben.

6.13 Rettungsdienst wird neu organisiert

Der Rettungsdienst in Bremen soll neu organisiert werden. Dazu wurde eine Untersuchung in Auftrag gegeben.

Mit der Erstellung eines entsprechenden Gutachtens wurde eine auswärtige Firma beauftragt. Dabei wurde ich beteiligt und um Darlegung datenschutzrechtlicher Kriterien für diese Untersuchung gebeten. Diesem Wunsch bin ich nachgekommen und habe einige den Datenschutz gewährleistende Hinweise und Anregungen gegeben. So sind bereits in einer frühen Untersuchungsphase personenbezogene Daten von „Patienten“ und Mitarbeitern des Rettungsdienstes zu anonymisieren bzw. erforderlichenfalls zu pseudonymisieren. Die erforderlichen Daten werden dem Gutachter in aufbereiteter Form zur Verfügung gestellt.

6.14 Private Daten im Zugriff

Mit einer Eingabe beklagte ein Mitarbeiter der Feuerwehr Bremen, dass eine von ihm erstellte private Datei in einem Verzeichnis aufgetaucht sei, die auch anderen Kollegen des Sachgebietes zugänglich sei. Ich habe den Vorfall untersucht und die Dateiverwaltung bei der Feuerwehr in Bremen geprüft.

Es wurde dargestellt, dass es für jeden Mitarbeiter Zugriffsmöglichkeiten auf Dateien des ihm zugeordneten Sachgebietes gibt. Weiterhin verfügt jeder Anwender über einen sogenannten „privaten“ Dateiordner, in welchem er eigene Dateien ablegen kann. Im Gespräch mit dem Datenschutzbeauftragten der Feuerwehr und den Administratoren wurde allerdings deutlich, dass es über den Begriff der „privaten“ Dateien und den Umgang mit dem entsprechenden Verzeichnis keine klaren Regelungen und Aussagen gibt. Während der Eingeber offensichtlich davon ausging, er könne hier private Dateien ohne dienstlichen Bezug speichern, verstanden die Verantwortlichen der Feuerwehr den Begriff der privaten Dateien im Sinne von „Daten eines Mitarbeiters mit dienstlichem Bezug“.

Die in dieser Eingabe betroffene private Datei wurde bei Auffinden gelöscht. Es ließ sich nachträglich nicht mehr klären, ob der Eingeber selbst die Datei versehentlich auf einem durch sein Sachgebiet allgemein zugänglichen Laufwerk abgelegt oder ob hier ein missbräuchlicher Zugriff auf Daten stattgefunden hat.

Meine Fragen bzgl. der Rechtevergabe auf Verzeichnisse und bzgl. der Protokollierung wurden bisher nicht beantwortet. Ich stehe diesbezüglich mit dem behördlichen Datenschutzbeauftragten der Feuerwehr in Kontakt. Ziel ist die Erhöhung der Transparenz bei der Bearbeitung und Administration von Dateien. Bei Erlaubnis der Bearbeitung privater Dateien, aber auch zum Schutz anderer sensibler personenbezogener Daten (z. B. beim Personalrat) sollten geeignete Möglichkeiten zur Verschlüsselung der Dateien zur Verfügung gestellt werden. Es sind klare Regelungen für die Mitarbeiter der Feuerwehr im Umgang mit dienstlichen und privaten Dateien zu machen. Diese sind den Mitarbeitern zur Kenntnis zu geben.

6.15 Dakota bei der Feuerwehr

Die Feuerwehr Bremen möchte zukünftig zur Abrechnung von Leistungen im Rettungsdienst durch ihre Rechnungsstelle Abrechnungsdaten zu Krankenkassen übertragen und hat sich vor Einführung entsprechender Software mit mir in Verbindung gesetzt. Für die Übertragung und Verschlüsselung soll das Produkt dakota.le eingesetzt werden.

Dakota.le (Datenaustausch und Kommunikation auf Basis Technischer Anlagen) ist ein Produkt der „Informationstechnischen Servicestelle der gesetzlichen Krankenkassen GmbH“ (ITSG), welche im Auftrag aller Spitzenverbände der Krankenkassen Aufgaben zur Vorbereitung, Realisierung und Optimierung der Datenaustauschverfahren übernimmt, dafür spezielle Produkte und Dienstleistungen anbietet und ein Trustcenter betreibt.

Die zu übertragenden Abrechnungsdaten entstehen bei den Einsätzen der Feuerwehr z. B. bei einem Krankentransport oder Rettungseinsatz. Die Datensätze beinhalten unter anderem folgende Angaben: Name, Vorname und Geburtsdatum des Patienten sowie Versicherungsnehmer, Krankenkasse, Art und Grund des Einsatzes.

Die Teilnahme an diesem Verfahren ist durch den Antrag auf Zertifizierung bei einem Trustcenter möglich. Zum Schutz der personenbezogenen Daten findet auf dem Übertragungsweg eine Verschlüsselung statt. Die Authentizität wird von einer neutralen Stelle, dem Trustcenter, durch ein Zertifikat bestätigt.

Das Produkt dakota.le soll in das Abrechnungssystem der Feuerwehr integriert werden. Der erste Entwurf einer Verfahrensbeschreibung der Feuerwehr Bremen ist bei mir eingegangen. Es steht allerdings noch eine genauere Beschreibung der technischen und organisatorischen Maßnahmen (Sicherheitsrichtlinien) zur Absicherung des Verfahrens und insbesondere der Teilnehmerschlüssel aus.

Sobald Programmversionen mit Erweiterungen und Verbesserungen bezüglich der Verschlüsselung (z. B. Erhöhung der Schlüssellänge) oder Einsatz einer qualifizierten digitalen Signatur mit Chipkarte herausgegeben werden, sind diese zur weiteren Erhöhung des Schutzniveaus einzusetzen.

Die Einführung dieser Software wird weiter von mir verfolgt. Die Bewertung ist noch nicht abgeschlossen.

7. Justiz

7.1 Großer Lauschangriff in weiten Teilen verfassungswidrig

Im Jahr 1998 wurden durch eine Grundgesetzänderung in Art. 13 GG - dem Grundrecht auf Unverletzlichkeit der Wohnung - die Absätze 3 bis 6 eingefügt. Nach Art. 13 Abs. 3 GG ist eine akustische Wohnraumüberwachung zum Zwecke der Strafverfolgung möglich. In § 100c Abs. 1 Nr. 3 Strafprozessordnung (StPO) erhielt der große Lauschangriff seine einfachgesetzliche Legitimation. Hiernach durfte das in einer Wohnung nichtöffentlich gesprochene Wort eines Beschuldigten durch die Strafverfolgungsbehörden abgehört und aufgezeichnet werden, wenn bestimmte Tatsachen den Verdacht begründeten, dass er eine der näher bezeichneten Katalogtaten begangen hatte.

Das Bundesverfassungsgericht (BVerfG) hat am 3. März 2004 entschieden, dass die gesetzliche Regelung in der Strafprozessordnung zum großen Lauschangriff in weiten Teilen verfassungswidrig ist.

Nach dem Bundesverfassungsgericht sollen nur noch solche Maßnahmen zulässig sein, welche die Menschenwürde wahren. Der Kernbereich privater Lebensgestaltung ist vor akustischen Überwachungsmaßnahmen zu schützen.

Das Gericht hat den Artikel 13 GG Abs. 3 als solchen nicht für verfassungswidrig erklärt, sondern im Wege der systematischen Verfassungsauslegung weitere ungeschriebene Grenzen hinzugefügt:

- Abhörmaßnahmen sind dann zu unterlassen, wenn sich jemand allein oder mit Personen seines Vertrauens in der Wohnung aufhält und keine konkreten Anhaltspunkte dafür bestehen, dass die zu erwartenden Gespräche einen unmittelbaren Bezug zu Straftaten aufweisen. Im Zweifel ist für die Privatsphäre zu entscheiden.
- Der Kernbereich privater Lebensgestaltung muss durch Erhebungs- und Verwertungsverbote konkretisiert werden. Bei Rechtswidrigkeit der Erhebung muss die Maßnahme abgebrochen und die Aufzeichnungen müssen vernichtet werden.
- Anlasstaten müssen bei abstrakter Betrachtung besonders schwerwiegend sein. Die Höchststrafe muss über fünf Jahre Freiheitsstrafe liegen.
- Art, Dauer und Umfang der Maßnahme sind in einer richterlichen Anordnung eingehend zu begründen.
- Es bestehen Benachrichtigungspflichten. Grundsätzlich sind auch Drittbetroffene zu benachrichtigen.

Da die Regelungen in der Strafprozessordnung diesen Anforderungen nicht entsprechen, hat das Bundesverfassungsgericht sie zu großen Teilen für verfassungswidrig erklärt. Der Bundesgesetzgeber wurde durch das Gericht verpflichtet, bis spätestens zum 30. Juni 2005 einen verfassungsmäßigen Zustand herzustellen.

Im September 2004 hat die Bundesregierung einen Gesetzentwurf beschlossen, der die vom Bundesverfassungsgericht geforderten Einschränkungen bei der akustischen Wohnraumüberwachung umsetzen soll. Allerdings sind zentrale Punkte, wie die Begriffsbestimmung des „unantastbaren

Kernbereichs der privaten Lebensgestaltung“ und die Bestimmung des Kreises der Menschen des „persönlichen Vertrauens“ offen geblieben. Die Konferenz der Datenschutzbeauftragten hat im März 2004 eine Entschließung (vgl. Ziff. 15.4 dieses Berichts) verabschiedet, in welcher sie weitergehende Konsequenzen aus dem Urteil des Bundesverfassungsgerichts fordert. Diese Forderung wurde nochmals in einer Entschließung der Konferenz im Oktober 2004 (vgl. Ziff. 15.7 dieses Berichts) bekräftigt.

Darüber hinaus beschränken sich die Auswirkungen des Bundesverfassungsgerichtsurteils nicht nur auf die akustische Wohnraumüberwachung. Vielmehr stehen auch andere Eingriffsbefugnisse, wie etwa die Telekommunikationsüberwachung und andere Formen der verdeckten Datenerhebung mit zwangsläufigen Berührungen des Bereichs privater Lebensgestaltung, auf dem Prüfstand.

7.2 Datenschutz im Notariat

Ich habe bei verschiedenen zufällig ausgewählten Notaren die technische Umgebung der Büros untersucht, um aus der praktischen Erfahrung heraus allgemeine Empfehlungen zur Verbesserung des Datenschutzes geben zu können. Aufgrund der bestehenden Geheimhaltungspflichten und der Sensibilität der dort verarbeiteten Daten, z. B. in Grundstücksverträgen oder Testamenten, sind gerade bei Notariaten besonders hohe Anforderungen an den Datenschutz zu stellen. Schwerpunkt der Prüfung war die Einhaltung der technischen und organisatorischen Maßnahmen gemäß § 7 Bremisches Datenschutzgesetz (BremDSG).

Die Qualität des Datenschutzes war von Notariat zu Notariat sehr unterschiedlich. Bei den nachstehend dargestellten Schwachstellen handelt es sich lediglich um eine Zusammenfassung aller während der einzelnen Prüfungen festgestellten Mängel.

Aus den Prüfergebnissen habe ich folgende Anforderungen formuliert:

Server dürfen nicht frei zugänglich sein. Unbefugten ist nach § 7 Abs. 4 Nr. 1 Bremisches Datenschutzgesetz (BremDSG) der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (sog. Zutrittskontrolle). Außerdem ist nach § 7 Abs. 4 Nr. 2 BremDSG zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (sog. Zugangskontrolle). Aus diesem Grund sollten Server in abschließbaren Räumen oder verschließbaren Schränken stehen.

Bei der Verwendung von Spezialsoftware für Notariate sind die Aufgaben des Notariats von denen der Rechtsanwaltskanzlei zu trennen. Das kann z. B. durch eine Anpassung der Zugriffsrechte oder nur teilweise Installation der Module gewährleistet werden, da dann nur auf die für die entsprechende Aufgabe erforderlichen Daten zurückgegriffen werden kann. Eine fehlende Trennung stellt einen Verstoß gegen den Zweckbindungsgrundsatz des § 12 Abs. 1 BremDSG dar.

Wichtig ist es auch, dass Mitarbeiterinnen und Mitarbeiter der Notare den Aufgaben entsprechende Rollen bzw. Zugriffsrechte sowohl auf Betriebssystemebene als auch innerhalb eventuell eingesetzter Spezialsoftware zugewiesen werden können. Dies entspricht § 7 Abs. 4 Nr. 3 BremDSG und ermöglicht differenzierte Schreib- und Leserechte auf Datenbestände und Anwendungen.

Bei Internet- und E-Mail-Nutzung müssen umfangreiche Maßnahmen zum Schutz von Vertraulichkeit, Integrität und Authentizität der Daten getroffen werden. Datenverarbeitungssysteme, die zu anderen Netzen wie z. B. dem Internet hin geöffnet werden, sind gegenüber diesen Netzen durch geeignete Maßnahmen abzuschotten, beispielsweise durch den Einsatz einer Firewall. Ein Datenaustausch per E-Mail darf nur erfolgen, wenn dieser mit einem sicheren Verfahren verschlüsselt wird.

Problematisch stellt sich auch eine Fernwartung dar. Bei dieser handelt es sich rechtlich gesehen um eine Datenverarbeitung im Auftrag i. S. v. § 9 BremDSG. Hiernach ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig vom Auftraggeber (dem Notar) auszuwählen. Sofern das Bremische Datenschutzgesetz auf den Auftragnehmer keine Anwendung findet, ist der Auftraggeber verpflichtet,

vertraglich sicherzustellen, dass der Auftragnehmer die Vorschriften des Bremischen Datenschutzgesetzes beachtet und sich der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft.

Technisch gesehen bedeutet Fernwartung immer eine Öffnung der Netze „nach außen“. Daher sind entsprechende technische und organisatorische Maßnahmen zu treffen, um die Fernwartung dem Stand der Technik entsprechend sicher zu gestalten. Fernwartung darf nur angemeldet (z. B. durch einen vorherigen ankündigenden Anruf) erfolgen, ggf. ist der Fernwartungszugang zum System so zu realisieren, dass nur im Bedarfsfall von der Seite des Notariats die Möglichkeit geschaffen wird, dass eine Einwahl zur Fernwartung von außen möglich ist.

Auch der Einsatz funkbasierter Systeme nimmt immer weiter zu. Funkbasierte Systeme öffnen bestehende kabelbasierte Netze. Die Angriffsmöglichkeiten auf das Netz und die gespeicherten und verarbeiteten Daten sind in solchen Fällen vielfältig. Es ist daher ein erhöhter Aufwand zur Abschottung und Absicherung des Netzes zu betreiben, wenn funkbasiert arbeitende Komponenten eingesetzt werden.

Die vorstehend dargestellten Schwachpunkte zeigen, dass eine kompetente Beratung nicht entbehrlich ist. Zur Sicherstellung der Einhaltung der datenschutzrechtlichen Bestimmungen soll die Bestellung eines behördlichen Datenschutzbeauftragten gemäß § 7 a BremDSG beitragen. Aus diesem Grund habe ich die Notarkammer angeschrieben und gebeten, ihre Mitglieder über die gesetzliche Verpflichtung zu unterrichten.

7.3 Veröffentlichungen von Insolvenzbekanntmachungen im Internet

Leider bestehen die bereits in meinem 26. Jahresbericht aufgezeigten datenschutzrechtlichen Defizite bei Veröffentlichungen von Insolvenzbekanntmachungen im Internet weiterhin. Der Kopierschutz in einem bundesweiten Register ist nicht ausreichend. Mittlerweile veröffentlichen 14 Bundesländer ihre Bekanntmachungen über Verbraucherinsolvenzen auf der gemeinsamen Internetseite www.insolvenzbekanntmachungen.de. Der Internetauftritt wird aufgrund einer Verwaltungsvereinbarung vom Justizministerium Nordrhein-Westfalen betreut.

Die Veröffentlichung im Internet ist zwar kostengünstiger, birgt aber auch erhebliche Gefahren für das Recht auf informationelle Selbstbestimmung der Betroffenen. So besteht insbesondere die Gefahr, dass Schuldner für den Rest ihres Lebens unkontrolliert in privaten Dateien oder Datenbanken registriert werden, selbst wenn die amtlichen Löschfristen schon längst abgelaufen sind.

Der Gesetzgeber hat angesichts dieser Gefahrenlage gesetzliche Regelungen geschaffen. Hierdurch soll einer Speicherung und Verbreitung durch Dritte entgegengewirkt werden. § 9 Abs. 2 Satz 3 Nr. 3 Insolvenzordnung (InsO) und § 2 Abs. 1 Satz 3 der entsprechenden Verordnung verlangen, dass die Veröffentlichungen nach dem Stand der Technik durch Dritte nicht kopiert werden können. In der Praxis der Veröffentlichungen im Internet wird der gesetzlich geforderte Kopierschutz aber nicht eingehalten. Zwischenzeitlich hat sich der Rechtsausschuss für die Problematik interessiert, er will sich im kommenden Berichtsjahr erneut hiermit befassen. Ich habe technische Lösungen aufgezeigt, durch welche ein Kopierschutz erreicht werden kann. Der Senator für Justiz und Verfassung hat diese Lösungsvorschläge an das Justizministerium Nordrhein-Westfalen weitergeleitet.

Darüber hinaus führt die gemeinschaftliche Veröffentlichung von Insolvenzdaten durch die Länder wegen der Möglichkeit der „uneingeschränkten Suche“ zu erheblich größeren Ergebnislisten als bei einer regionalen Veröffentlichung. Eine Beschränkung des Angebots auf eingeschränkte Suchabfragen wäre aus datenschutzrechtlicher Sicht wünschenswert.

7.4 Beratung von Forschungsvorhaben im Justizbereich

Um im Justizbereich die Einhaltung von datenschutzrechtlichen Vorschriften zu erleichtern, habe ich in meinem Hause in Abstimmung mit dem Justizressort ein Merkblatt für den Datenschutz bei Forschungsprojekten entwickelt, welches den betroffenen Behörden übersandt wurde. Anlass war mein Bericht im 26. Jahresbericht über ein Forschungsvorhaben im Justizbereich (vgl. Ziff. 7.5), bei dessen Durchführung die datenschutzrechtlichen Vorschriften völlig unzulänglich beachtet worden sind. In diesem Zusammenhang hatte ich auch bemängelt, dass ich nicht in das Verfahren mit einbezogen worden bin.

In diesem Berichtsjahr wurden mir mehrere Forschungsvorhaben aus dem Justizbereich in der Vorbereitungsphase zugeleitet, so dass ich die Möglichkeit zur Stellungnahme hatte. Die Zusammenarbeit war konstruktiv, die von mir geäußerten datenschutzrechtlichen Korrekturwünsche und Verbesserungsvorschläge wurden in den einzelnen Projekten umgesetzt.

8. Gesundheit und Krankenversicherung

8.1 Stoffwechselscreening bei Neugeborenen

Eine weitere – und schon seit längerem durchgeführte – flächendeckende Untersuchung bei Neugeborenen ist das Stoffwechselscreening. Dabei handelt es sich um eine Blutuntersuchung zur Erkennung schwerwiegender Stoffwechselerkrankungen, die, frühzeitig erkannt, behandelbar sind. Dem Neugeborenen wird ein Blutstropfen aus der Ferse entnommen, der auf eine Testkarte aufgebracht wird. Die Karte hat neben dem Teil für die Blutprobe auch einen Abschnitt mit den Identitätsdaten des Kindes. Die Stoffwechseluntersuchungen werden im gesamten Bundesgebiet durchgeführt; die Proben aus Bremen werden im Labor des Universitätsklinikums Hamburg-Eppendorf untersucht. Dort werden die Blutproben und die personenbezogenen Daten nach Ablauf von sechs Monaten mittels Vergabe einer Codenummer pseudonymisiert und nach Ablauf von fünf Jahren wird der personenbezogene Teil der Blutproben vernichtet.

Ich habe den Senator für Gesundheit darauf aufmerksam gemacht, dass für die Verarbeitung von Daten aus Bremer Kliniken in dem Hamburger Labor eine schriftliche Vereinbarung über die Auftragsdatenverarbeitung gemäß § 9 Bremisches Datenschutzgesetz (BremDSG) erforderlich ist. Zurzeit laufen allerdings Beratungen über den Entwurf einer neuen Kinderrichtlinie des Gemeinsamen Bundesausschusses, der auch eine Regelung des Stoffwechselscreenings bei Neugeborenen umfasst. Möglicherweise wird diese Vorsorgeuntersuchung in die Regelversorgung der Gesetzlichen Krankenversicherung (GKV) aufgenommen. Diese Entwicklung wird vom Bundesbeauftragten für den Datenschutz (BfD) begleitet. Der Senator für Gesundheit sieht sich daher derzeit nicht in der Lage, eine bremische Regelung zur Auftragsdatenverarbeitung zu treffen, denn es werde in Kürze eine verbindliche Entscheidung des Gemeinsamen Bundesausschusses mit konkreten Vorgaben auch zum Datenschutz erwartet. Es bleibt abzuwarten, ob die erwarteten Regelungen insbesondere auch Aussagen darüber enthalten werden, wie mit den bisher vorhandenen Altdaten umzugehen ist. Anderenfalls wäre zumindest dafür eine Vereinbarung auf Landesebene zu treffen.

8.2 Hörscreening bei Neugeborenen

Im Berichtsjahr wurde in Bremen eine flächendeckende Untersuchung der Hörfähigkeit bei Neugeborenen, das sogenannte Hörscreening, eingeführt. Mit der Untersuchung wird das Ziel verfolgt, angeborene oder während der Schwangerschaft erworbene Hörstörungen zu erkennen und so eine frühzeitige Behandlung des Kindes und damit eine normale Sprachentwicklung zu ermöglichen (vgl. 26. JB, Ziff. 8.1.2).

Derzeit ist das Screening als freiwilliges, kostenfreies Angebot ausgestaltet. Die Eltern bekommen ein Informationsblatt über das Hörscreening. In der Regel wird die Untersuchung durchgeführt und im Vorsorgeheft eingetragen. Eine Ablehnung durch die Eltern muss aus haftungsrechtlichen Gründen ebenfalls dokumentiert werden. Eine elektronische Erfassung der aus den Untersuchungen gewonnenen Daten erfolgt bisher nicht. Die Einführung eines Systems zur Durchführung eines Follow-up (Tracking) und zur Qualitätssicherung wird von den Beteiligten als wünschenswert erachtet, befindet sich aber erst in der Planungsphase. Das Follow-up, also die Nachverfolgung der untersuchten Kinder durch die screenende Stelle, wird deshalb für notwendig gehalten, weil bei auffälligem Befund nicht immer sichergestellt sei, dass die Eltern das Angebot zur Nachuntersuchung wahrnehmen. Diese Funktion wird derzeit von den niedergelassenen Ärzten übernommen. Den Eltern von auffällig gescreenten Kindern wird eine Liste mit HNO-Ärzten/Pädaudiologen übergeben mit dem Hinweis, eine Nachuntersuchung durchführen zu lassen. Ebenso soll die Dokumentation im Vorsorgeheft dazu dienen, den Kinderarzt aufmerksam zu machen, falls der Eintrag, dass ein Hörtest durchgeführt wurde, fehlt.

Hinsichtlich der Einführung eines Erfassungsmodells für das Hörscreening beriet ich die Beteiligten dahingehend, dass zur weiteren Verarbeitung der Daten eine Einwilligung der Eltern erforderlich und für das Verfahren eine Pseudonymisierung der Untersuchungsergebnisse vorzusehen sei. Ich werde das Vorhaben weiter datenschutzrechtlich begleiten.

8.3 Gentests bei Neugeborenen und Gendatenbanken

Alarmiert durch Meldungen der Presse, die EU plane Gentests für alle Neugeborenen, sah ich mich veranlasst, den Hintergründen dieser Nachricht nachzugehen.

Festzuhalten ist zunächst, dass die EU keine verpflichtenden Regelungen zur Einführung medizinischer Untersuchungen in den Mitgliedstaaten treffen kann. Die Pressemeldung bezog sich auf eine Empfehlung des EU-Forschungskommissars Busquin, die im Rahmen einer Konferenz zu verantwortungsvoller und ethisch vertretbarer Anwendung von Gentests ausgesprochen wurde.

In verschiedenen Zeitungen wurde dabei von einem Screening, das per Gentest bei Neugeborenen durchgeführt werden soll, berichtet. Ein Screening beinhaltet die reihenweise Untersuchung einer bestimmten Gruppe auf eine oder mehrere definierte Krankheiten. Gegenwärtig wird bei Neugeborenen bereits ein Screening auf schwere, behandelbare Stoffwechselkrankheiten durchgeführt. Bei dem bisherigen Neugeborenen-Screening wird keine genetische Untersuchung durchgeführt. Hintergrund für die Forderung einer Erweiterung der Untersuchung auf genetische Tests ist, dass bestimmte Krankheiten nur so erkannt werden können.

Dass die Vorstellung, Säuglinge würden reihenweise genetisch untersucht, im Hinblick auf die vielfältigen Verwendungsmöglichkeiten dieser Daten Unbehagen auslöst, ist verständlich. Schließlich enthalten die Gene die gesamten Erbinformationen des Kindes wie auch Informationen über die genetische Konstellation der Eltern. Daher ist es von besonderer Bedeutung, für ein solches Verfahren klare Regelungen zu treffen, um die Wahrung des informationellen Selbstbestimmungsrechts der Betroffenen zu gewährleisten. Neben dem Recht, Informationen über die eigene Person zu kennen, gehört im medizinischen Bereich auch das Recht auf Nichtwissen dazu. Mittels genetischer Untersuchungen können Dispositionen zu Krankheiten festgestellt werden, deren Ausbruch nicht gewiss ist bzw. erst in späteren Lebensjahren stattfinden wird. Dies kann eine erhebliche Belastung für die Betroffenen aber auch für Eltern in Bezug auf ihr Kind bedeuten. Meine datenschutzrechtliche Forderung ist daher, dass bei Neugeborenen nur auf behandelbare Krankheiten untersucht wird.

Der in die Kritik geratene EU-Forschungskommissar stellte klar, dass die Teilnahme an dem Screening mittels Gentest freiwillig sein soll. Dabei zu bedenken ist allerdings, dass das Kind bei schweren, behandelbaren Krankheiten möglicherweise einen Anspruch auf die Untersuchung und Behandlung hat. Hinzu treten könnten moralische Konflikte bei den Eltern. Eine Lösung wäre, die Untersuchung als Standard in den Behandlungsvertrag über die Geburt aufzunehmen. Eine qualifizierte Information der Eltern über das Screening ist in jedem Fall erforderlich. Wird der Durchführung des Screenings widersprochen – eine zwangsweise Untersuchung kann es nicht geben – bliebe den Ärzten nur, dies zu dokumentieren.

Wie bereits bei dem herkömmlichen Screening-Verfahren stellt sich hier besonders das Problem der Aufbewahrung des bei dem Test entnommenen genetischen Materials. Es ist festzulegen, wo und wie lange aufbewahrt wird und vor allem, wann der Personenbezug abgetrennt, die Proben also anonymisiert werden. Denn wenn auch bei Durchführung der Untersuchung eine Einwilligung der

Eltern vorliegt, so hat das Kind, das später einmal selbst einwilligungsfähig ist, ein solches Einverständnis über die Erhebung und Speicherung seiner genetischen Informationen nicht gegeben.

Besondere Aufmerksamkeit verdient aus datenschutzrechtlicher Sicht das Vorhaben, genetische Daten zu Forschungszwecken in Datenbanken einzuspeisen. Eine solche Datenerfassung kann nur anonymisiert erfolgen und bedarf einer auf der Basis wissenschaftlicher und gesundheitspolitischer Erkenntnisse entwickelten gesetzlichen Regelung. Festzuhalten bleibt, dass die von Herrn Busquin ausgesprochene Empfehlung Aufsehen erregt hat, vieles in Bezug auf die Umsetzung eines genetischen Screenings aber noch ungeklärt ist.

Dass dieses Thema weiter an Aktualität gewinnt, zeigt sich auch an dem jüngst durch die Bundesgesundheitsministerin vorgelegten Gesetzentwurf „über genetische Untersuchungen am Menschen“. Damit soll per gesetzlicher Regelung sichergestellt werden, dass niemand wegen seiner genetischen Eigenschaften benachteiligt wird. Gefahren dieser Art bestehen insbesondere, wenn es darum geht, Versicherungs- oder Arbeitsverträge abzuschließen. Daher dürfen nach dem Gesetzentwurf Arbeitgeber von Bewerbern Gentests weder verlangen noch annehmen. Eine Ausnahme soll allerdings für Berufe mit gesundheitsgefährdenden Tätigkeiten gelten. Auch bei Lebens-, Pflege- und Berufsunfähigkeitsversicherungen ist eine Ausnahme vorgesehen, und zwar soll die Vorlage bereits vorhandener Gentests ab einer bestimmten Versicherungssumme verlangt werden dürfen. Bei genetischen Untersuchungen soll die Beratung durch einen Mediziner obligatorisch sein. Genetische Untersuchungen zu Forschungszwecken sollen nur mit der informierten Zustimmung der Betroffenen zulässig sein. Die Frage, wie mit Personen umzugehen ist, die nicht einwilligen können, wird noch zu diskutieren sein.

Eine gesetzliche Regelung von genetischen Untersuchungen am Menschen hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits in ihrer Entschließung im Jahr 2001 gefordert. Insbesondere sind danach Regelungen für genetische Untersuchungen zu medizinischen Zwecken, zur Klärung von Identität und Abstammung, im Zusammenhang mit Arbeits- und Versicherungsverhältnissen sowie zu Forschungszwecken zu treffen. Hervorgehoben wird dabei auch die besondere Bedeutung des Informations- und Entscheidungsrechts der betroffenen Personen.

Ich unterstütze die Initiative, den Schutz der Informationen über das Erbgut gesetzlich zu garantieren, und werde mich weiter an der Diskussion beteiligen.

8.4 Überprüfung des Hilfesystems für psychisch Kranke durch externen Gutachter

Das bremische Hilfesystem für psychisch Kranke geriet in die öffentliche Kritik, als nach einem Tötungsdelikt Hinweise bekannt wurden, dass von dem Täter, der bereits mehrfach in psychiatrischer Behandlung war, eine Gefahr ausgehen könnte, eine Reaktion darauf aber - möglicherweise aus organisatorischen Mängeln - unterblieben sei. Nun soll ein externer Gutachter die Organisation des Hilfesystems untersuchen. Dabei wird auch Einblick in Patientenunterlagen des Gesundheitsamtes genommen werden müssen.

In diesem Zusammenhang machte ich den Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales auf die Belange des Datenschutzes in dieser Angelegenheit aufmerksam. Ich gab zu bedenken, dass eine Einsichtnahme in personenbezogene Krankenunterlagen zu vermeiden ist und bat um weitere Unterrichtung in dieser Sache. Nunmehr wurde bekannt, dass der in Aussicht genommene Gutachter aufgrund seiner Verbindung zu einigen Beteiligten nicht in Betracht käme. Die Durchführung der Begutachtung befindet sich somit noch in der Planungsphase. Ich werde weiter darauf hinwirken, dass bei dem Vorhaben, bei dem sensible Gesundheitsdaten wie auch Arbeitnehmerdaten betroffen sein können, dem Datenschutz Rechnung getragen wird.

8.5 Mammographie-Screening

Die Brustkrebs-Früherkennung wird ab 2005 in die Regelversorgung der Gesetzlichen Krankenversicherung (GKV) übernommen. Grundlage dafür sind die Krebsfrüherkennungsrichtlinien des Bundesausschusses der Ärzte und Krankenkassen. Bisher wurden diese Vorsorgeuntersuchungen u. a. in Bremen in Modellprojekten erprobt. Ab April 2005 wird dann das Bremer Modellprojekt in die Regelversorgung übergehen, und zwar gemeinsam mit Niedersachsen. Dazu wurde eine Kooperationsvereinbarung geschlossen. In den Richtlinien sind so genannte zentrale Stellen vorgesehen, die das Einladewesen koordinieren. Dies wird das Gesundheitsamt Bremen gemeinsam für Bremen und Niedersachsen sein, das bereits bisher die Aufgabe der einladenden Stelle im Rahmen des Modellprojekts wahrgenommen hat. Das Gesundheitsamt Bremen wird also alle Frauen im Alter zwischen 50 und 69 Jahren in Bremen und Niedersachsen anschreiben und zu Vorsorgeuntersuchungen einladen, die dann in nahe gelegenen Praxen, die sich für die Teilnahme an den Screening-Untersuchungen qualifiziert haben, durchgeführt werden können. Hierfür wird eine Änderung der Meldegesetze beider Länder erforderlich, da das Gesundheitsamt Bremen nun auch Daten der Einwohnerinnen Niedersachsens von den Einwohnermeldeämtern erhalten soll, und zum anderen die in Bremen bisher bestehenden Regelungen auf das Modellprojekt begrenzt und im Rahmen der Regelversorgung unzureichend waren (vgl. 26. JB, Ziff. 8.2.2.2). Dazu wurde eine Änderung der bremischen Meldedatenübermittlungsverordnung bezüglich der im Rahmen der Regelversorgung vorgesehenen Datenübermittlungen mit mir abgestimmt. Daneben prüfe ich derzeit ein Datenschutzkonzept, das mir seitens des Gesundheitsamts Bremen als zentrale Stelle vorgelegt wurde.

8.6 Bremer Krebsregister und Tumornachsorgeleitstelle

Das Krebsregister setzt sich zusammen aus der ärztlich geleiteten Vertrauensstelle und der gemäß § 1 Abs. 3 des Gesetzes über das Krebsregister der Freien Hansestadt Bremen (BremKRG) hiervon räumlich, organisatorisch und personell getrennten epidemiologischen Registerstelle zur statistischen Erfassung von Krebserkrankungen. Auf die Einhaltung dieser strikten Trennung habe ich stets in tatsächlicher und technischer Hinsicht besonderes Augenmerk gelegt. Daneben gibt es ein klinisches Krebsregister, die Tumornachsorgeleitstelle, das, im Gegensatz zu den rein statistischen Aufgaben des epidemiologischen Registers, Daten über Krankheitsverlauf und Therapie erfasst. Auch die Nachsorgeleitstelle muss von den anderen Einrichtungen des Krebsregisters getrennt sein. Die Überprüfung der Einhaltung dieser Maßgabe war insbesondere deshalb von Bedeutung, da sich Vertrauensstelle und Tumornachsorgeleitstelle Räumlichkeiten im Gebäude der Kassenärztlichen Vereinigung Bremen teilten.

Wegen der Beendigung des Mietverhältnisses muss die Vertrauensstelle nun neue Räumlichkeiten beziehen. Die neuen Büroräume werden sich im Gebäude des Bremer Instituts für Präventionsforschung und Sozialmedizin (BIPS) befinden, das auch das epidemiologische Register führt. Hierbei waren in erster Linie die technischen Maßnahmen von Bedeutung, da über eine Trennung der Systeme die Einhaltung der datenschutzrechtlichen Vorgaben gewährleistet werden können.

Daneben erfuhr ich, dass die Tumornachsorgeleitstelle eventuell aus Kostengründen geschlossen werden muss. Ich teilte den Verantwortlichen mit, dass darauf zu achten sei, dass die vorhandenen Daten sicher aufbewahrt werden und die Auskunftsrechte Betroffener weiterhin erfüllt werden können sowie schließlich, dass eine ordnungsgemäße Löschung der Daten erfolgt. Dies wurde bereits zugesagt. Nunmehr war aber der Presse zu entnehmen, dass im Wege eines privaten Sponsorings die Aufrechterhaltung der Tumornachsorgeleitstelle eventuell doch möglich sein könnte. Dann wird darauf zu achten sein, ob die bisherigen Strukturen erhalten bleiben oder ob es datenschutzrelevante Veränderungen geben wird.

Umzug der Vertrauensstelle des Bremer Krebsregisters – technische Maßnahmen: Das bremische Krebsregistergesetz schreibt die räumliche, organisatorische und personelle Trennung (§ 1 Abs. 3) zwischen der ärztlich geleiteten Vertrauensstelle und der epidemiologischen Registerstelle vor.

Zweck der Aufteilung des Registers in diese beiden Stellen ist es, eine Identifizierung einzelner Patienten anhand der über sie gespeicherten medizinischen Daten zu verhindern.

Deshalb übermittelt die Vertrauensstelle der Registerstelle die ihr gemeldeten medizinischen Daten nur mit einer von ihr vergebenen Registriernummer. Der Registerstelle darf die Deanonymisierung, d. h. die Verknüpfung der medizinischen Daten mit den identifizierenden Daten des Patienten, nicht möglich sein (§ 6 Abs.1 Nr. 4 BremKRG/vgl. auch 22. JB, Ziff. 8, 23. JB, Ziff. 8.4.3).

Durch den Umzug der Vertrauensstelle in das Bremer Institut für Präventionsforschung und Sozialmedizin (BIPS), bei dem die Registerstelle angesiedelt ist, werden hohe Anforderungen an die

Trennung der Datenbestände gestellt. Ich habe darauf geachtet, dass diese Anforderungen technisch umgesetzt werden.

Die Vertrauensstelle wird ein eigenes Netz erhalten, dass physikalisch von demjenigen des BIPS und der Registerstelle getrennt ist. Das bedeutet, dass es über diesen Weg keine Möglichkeit gibt, von außen auf die Datenbestände der Vertrauensstelle zuzugreifen.

Die Verwaltung der Datenbank mit den gemeldeten Patientendaten wird ausschließlich durch eine Mitarbeiterin der Vertrauensstelle wahrgenommen. Die Zugriffe auf die Datenbanken sind eindeutig definiert und auf die Mitarbeiterinnen der Vertrauensstelle beschränkt. Aus EDV-technischer Sicht ist somit die gesetzlich geforderte Trennung zur Registerstelle gewährleistet.

8.7 Elektronische Gesundheitskarte

Auf der Grundlage des Gesetzes zur Modernisierung der Gesetzlichen Krankenversicherung (GMG), das am 1. Januar 2004 in Kraft getreten ist, soll die bisherige Krankenversichertenkarte ab 2006 durch die elektronische Gesundheitskarte abgelöst werden. Neben ihren administrativen Funktionen soll die elektronische Gesundheitskarte auch Gesundheitsdaten aufnehmen. Die Karte wird daher als Chipkarte ausgestaltet sein, die geeignet ist, Authentifizierung, Verschlüsselung und elektronische Signatur zu ermöglichen. Außerdem soll sie mit einem Lichtbild des Versicherten versehen sein. Der medizinische Teil der elektronischen Gesundheitskarte, wie z. B. Notfalldaten oder Angaben über Untersuchungen und Diagnosen, soll nur auf freiwilliger Basis genutzt werden können.

Die Bremer Initiative „Telematik im Gesundheitswesen“ hat sich beim Bund als Testregion für die Einführung der Gesundheitskarte beworben. Zunächst bestand seitens des Bundesministeriums für Gesundheit und Soziale Sicherung (BMGS) die Überlegung, im Rahmen der Ausschreibung einen Zuschlag für einen oder mehrere Bewerber zu erteilen mit der Konsequenz, dass eine finanzielle Unterstützung des Projekts durch den Bund gewährt worden wäre. Nunmehr ist es in das Belieben der Länder gestellt, Testprojekte durchzuführen, sofern es den Ländern - auch in finanzieller Hinsicht - möglich ist.

Derzeit findet eine Akzeptanzstudie zur elektronischen Gesundheitskarte statt. Es ist angedacht, das in Bremen bereits existierende Projekt iBON (integratives Bremer Onkologie- und Hämatologie Netzwerk) zu erweitern, indem weitere Arztpraxen und Kliniken an das Netz angeschlossen werden und dieses Projekt in das Modellprojekt zur elektronischen Gesundheitskarte einfließen zu lassen. Auf Bundesebene sollen in Zusammenarbeit des BMGS und der Selbstverwaltung die technischen Spezifikationen erarbeitet werden; es wird eine Umsetzung bis März 2005 angestrebt. Dabei gibt es Überlegungen, die verschiedenen Aufgaben in den Testregionen arbeitsteilig zu erproben.

In jedem Fall sind die datenschutzrechtlichen Aspekte der elektronischen Gesundheitskarte eng mit den technischen Parametern verknüpft. Denn die Funktionen der Karte sind in § 291 a Sozialgesetzbuch (SGB) V festgelegt. Ob das dahinterliegende System der elektronischen Gesundheitskarte den Anforderungen des Datenschutzes genügen wird, hängt aber davon ab, wie die gesetzlichen Vorgaben technisch realisiert werden.

So ist beispielsweise zu gewährleisten, dass die Versicherten ihre Einsichts- und Auskunftsrechte gegenüber Ärzten geltend machen können. Auf der anderen Seite ist zu vermeiden, dass Versicherte dazu genötigt werden könnten, ihre Gesundheitsdaten anderen, z. B. Versicherungen oder Arbeitgebern, zu offenbaren. Daher wäre etwa die Ausgestaltung des Einsichtsrechts durch die Möglichkeit, die Karte einfach am heimischen PC zu lesen, problematisch. Andererseits muss gewährleistet sein, dass die Versicherten die Hoheit über ihre Daten haben und durch die Einführung der elektronischen Gesundheitskarte keine Schlechterstellung gegenüber der gegenwärtigen Situation eintritt.

Das alles zeigt schon: Für den Fall, dass Bremen Testregion wird, gilt es, ein Projekt von hoher technischer Komplexität zu begleiten.

So geht es unter vielen anderen Gesichtspunkten darum, wie die Datenhaltung gestaltet wird (zentral/dezentral oder als Mischform) und wie die Steuerung der Verfügbarkeit der Daten über eine datenschutzgerechte Zugriffslogik unter Einbeziehung der Chipkartentechnologie erfolgen soll.

Die Komplexität bezieht sich weiter auf Fragen der physikalischen und logischen Sicherheit, wie den Einsatz von Verschlüsselungs- und Authentifizierungsmechanismen.

Zur Unterstützung des Projektes „Elektronische Gesundheitskarte“ wurde vom BMGS ein aus mehreren Firmen bestehendes Projektkonsortium mit dem Namen „BIT4health“ beauftragt. Projektziel ist es, die bundesweite Einführung der elektronischen Gesundheitskarte vorzubereiten. Hierfür wurde u. a. eine „Solution Outline“ (letzte Version: 02.12.04) entwickelt, die eine zunächst grobe Definition einer Telematik- und Rahmenarchitektur sowie einer Sicherheitsinfrastruktur enthält.

Es werden innerhalb einer „Lösungsarchitektur“ (Betriebsorganisation) Sicherheitskomponenten wie beispielsweise zentrale Sicherheitsdienste und PKI (Public Key Infrastructure) im Gesundheitswesen beschrieben. Zur Erstellung der Lösungsarchitektur sind unter dem Gesichtspunkt der Sicherheitskomponenten eine Reihe von Aktivitäten und die Risiken für den Umsetzungsprozess definiert worden. Dazu gehören beispielsweise das Erstellen einer Bedrohungsanalyse, der Aufbau und die Festlegung der PKI-Struktur (die u. a. auch Grundlage für die elektronische Signatur ist), die Spezifikation zentraler und dezentraler Sicherheitsdienste.

Die Teststrategie, die sicherlich auch für Bremen von Bedeutung ist, ist bisher wenig konkret. Darin heißt es nur, dass detaillierte Testpläne und Testszenarien in der Planungs- und Designphase festgelegt werden. Als Testinhalte in Bezug auf die Sicherheitskomponenten werden der IPSec-Verbindungsaufbau mit Authentisierung über PKI und die Sicherheitsfunktionen für die zentralen Infrastrukturkomponenten und dezentral für die verschiedenen Zugangstechnologien genannt.

In Bremen müssten daher sowohl auf der Infrastrukturebene als auch im Detail auf der Anwendungsebene (beispielsweise die Differenzierung der Zugriffe auf Anwendungen oder einzelne Dokumente etc.) und auf beide Ebenen bezogen die Steuerungsmöglichkeiten über die Karte der Patientinnen und Patienten festgelegt werden.

Zunächst müssen die Zielkonflikte innerhalb der Kommunikationsbeziehungen zwischen Versicherten, Leistungserbringern und Kostenträgern gelöst werden. Erst dann kann die Datenschutztechnik zur Umsetzung dieser Lösungen eingesetzt werden.

Die Datenschutztechnik kann die Lösungen umsetzen, die innerhalb der Kommunikationsbeziehungen zwischen Versicherten, Leistungserbringern und Kostenträgern erzielt werden können.

Ich hoffe, dass in Bremen neben der Kompatibilität der Sicherheitskomponenten auch die „Kompatibilität“ der technischen Infrastruktur mit den Betroffenen, den Patienten, geprüft wird. Ist es tatsächlich möglich, die durch die Technik und Nutzung der Karte versprochene Selbstbestimmung und Eigenverantwortlichkeit zu realisieren? Welches Technikverständnis wird hier beim Einzelnen vorausgesetzt? Wie wird die Arzt-Patienten-Kommunikation beeinflusst oder gibt es innerhalb dieser Kommunikationsbeziehungen faktisch überhaupt eine Möglichkeit, die Gesundheitskarte steuernd einzusetzen, wo doch „Vertrauen“ Grundlage der Beziehung sein soll?

So ist in diesem spannenden und spannungsreichen Projekt die Wirkung des Datenschutzes sehr deutlich auch von sozialen und psychologischen Faktoren abhängig und muss immer zusammen mit den zur Verfügung gestellten technischen Möglichkeiten gesehen werden.

9. Arbeit und Soziales

9.1 Datenerhebung für das Arbeitslosengeld II

Bürgerinnen und Bürger, die bisher Hilfe zum Lebensunterhalt (HLU) nach dem Bundessozialhilfegesetz (BSHG) erhielten, wurden von den Sozialämtern angeschrieben und um Angaben für die Gewährung des Arbeitslosengelds II gebeten. Davon betroffen waren diejenigen Hilfeempfänger, die mindestens drei Stunden täglich erwerbsfähig sind. Dazu wurden die im Datenverarbeitungssystem PROSOZ vorhandenen Datensätze ausgewertet. Ich informierte mich bei den Sozialämtern der Stadtgemeinden Bremen und Bremerhaven über die in diesem Zusammenhang beabsichtigten Datenverarbeitungsvorgänge und versuchte, auf ein datenschutzgerechtes Vorgehen bei der Datenerhebung und der weiteren Verarbeitung hinzuwirken.

In Bremerhaven wurde zur Datenerhebung ausschließlich der 16-seitige Fragebogen der Bundesagentur für Arbeit (BA) verwendet. Auf die Daten aus den Sozialhilfeakten wurde nicht zurückgegriffen. In dem Informationsschreiben des Sozialamts wurde auf mein Betreiben den Betroffenen deutlich gemacht, wer die datenverarbeitende Stelle ist, der gegenüber die allgemeinen Betroffenenrechte – wie z. B. Auskunft, Sperrung, Löschung – geltend gemacht werden können, und dass diese besonders sensiblen, dem Sozialgeheimnis unterliegenden Daten nur für die Zwecke der Leistungsgewährung verarbeitet würden.

In der Stadtgemeinde Bremen hingegen wurde nicht der 16-seitige Fragebogen der BA verwendet, sondern es wurden die bisher aus dem Sozialhilfeverfahren vorhandenen Daten genutzt. Zur Erhebung der zusätzlich benötigten Informationen wurden die Anlagen 2 und 3 des von der BA konzipierten Fragebogens eingesetzt, die zusammen mit dem Kurzantragsformular und einem Informationsblatt versendet wurden. Darin wurden die Betroffenen über den Zweck der Datenerhebung und die Nutzung der bisher vorhandenen Daten informiert und darüber aufgeklärt, dass nach Abschluss der Ersterhebung der Daten für das Arbeitslosengeld II seitens der Sachbearbeitung nicht mehr auf die Daten aus der Sozialhilfeakte zugegriffen werde.

Es war Aufgabe der Sozialämter, den Betroffenen bei Bedarf Hilfestellung beim Ausfüllen der Fragebogen zu geben. In Bremerhaven entschloss man sich dazu, diese Aufgabe durch die Volkshochschule (VHS) wahrnehmen zu lassen. Die VHS übernahm es, die Betroffenen zu Kursen einzuladen; dazu wurden Namen und Anschriften der Betroffenen übermittelt. Die VHS vergab Unteraufträge zur Durchführung der Informationsveranstaltungen an drei privatrechtlich organisierte Stellen, die Wirtschafts- und Sozialakademie der Arbeitnehmerkammer, das Ausbildungsförderungszentrum im Land Bremen GmbH (AFZ) und die Akademie des Handwerks. Eine Einbeziehung Dritter ist nur nach den Regeln der Datenverarbeitung im Auftrag (§ 80 SGB X) zulässig. Bei den genannten Stellen führte ich eine Datenschutzprüfung durch und stellte datenschutzrechtliche Mängel fest. So sollten Listen über die Teilnahme an den Kursen erstellt werden, obwohl die Teilnahme freiwillig war. Ich forderte das Sozialamt Bremerhaven auf, die festgestellten Mängel umgehend abzustellen.

Auch der Rechtsausschuss der Bremischen Bürgerschaft interessierte sich für die Probleme bei der Datenverarbeitung. Auf seiner Sitzung am 22. September 2004 wurde vom Vertreter des Sozialamts

Bremerhaven erklärt, auf die Herstellung datenschutzgerechter Verhältnisse bei den Unterauftragnehmern hinzuwirken.

Kritik war auch an dem Zusatzblatt 2 des von der BA ausgegebenen Erhebungsbogens zu formulieren. Denn auf dessen Rückseite befand sich ein weiteres Antragsformular, das oftmals bereits vor der Vorlage beim Arbeitgeber mit persönlichen Daten ausgefüllt worden war. Zudem wurde dem Arbeitgeber damit deutlich, dass in der Familie des Arbeitnehmers ein Antrag auf Arbeitslosengeld II gestellt wurde. Dadurch wurden dem Arbeitgeber unnötig Sozialdaten offenbart. Aufgrund der Kritik der Datenschutzbeauftragten boten BA und BMWA ein separates Formblatt „Verdienstbescheinigung 2.1“ an, das auf der Homepage der BA abgerufen werden konnte und bei den Arbeitsagenturen vorgehalten wurde. Dieses sollte nach dem Ausfüllen durch den Arbeitgeber an das ursprüngliche Formular angeheftet werden, was letztlich bedeutete, dass das datenschutzrechtlich bedenkliche Zusatzblatt 2 weiterhin in hoher Auflage versendet wurde. Für Bremen und Bremerhaven konnte ich noch rechtzeitig erreichen, dass die Hinweise zum Umgang mit dem Zusatzblatt 2 in die Bürgerinformation aufgenommen wurden.

Weiter wurde eine Überarbeitung u. a. zur Vorlage des Mutterpasses, aus dem medizinische Daten hervorgehen, zur Angabe der Kontonummer des Vermieters sowie zu den Angaben zu den persönlichen Verhältnissen der mit dem Antragsteller in einem Haushalt lebenden Personen, notwendig. Die BA sagte Nachbesserung zu; diese könne allerdings erst in der nächsten Auflage der Bogen in 2005 umgesetzt werden, um die Auszahlung der ALG II-Leistungen nicht zu verzögern. Bis dahin sollen die Ausfüllhinweise den Betroffenen eine Hilfestellung bieten.

Festzuhalten bleibt, dass den Betroffenen eine Vielzahl sensibler Informationen über ihre persönlichen - insbesondere finanziellen - Verhältnisse abverlangt wurde. Die Abfrage dieser Daten ist aber Konsequenz der gesetzgeberischen Entscheidung zur Einführung des Arbeitslosengeldes II. Mit Blick auf eine rechtzeitige Leistungsgewährung war den Betroffenen trotz der datenschutzrechtlichen Mängel dennoch zu empfehlen, soweit nicht verbesserte Formulare zur Verfügung stehen, zunächst die bisherigen Formulare zu benutzen und in Zweifelsfragen die Ausfüllhinweise der BA zu Rate zu ziehen.

Die Daten für das Arbeitslosengeld II wurden auf der Grundlage des § 65 SGB II zunächst durch die Sozialämter erhoben. Ab 2005 bilden die Sozialämter mit der Agentur für Arbeit eine Arbeitsgemeinschaft nach § 44 b SGB II. In Bremen ist es die BAGIS.

9.2 Einführung des Verfahrens „A2LL“ in Bremen (Hartz IV)

Die Zugangssoftware zum Verfahren „A2LL“ (SGB **II** – **L**eistungen zum **L**ebensunterhalt) wurde in der Zeit vom 18. Oktober 2004 bis 25. Oktober 2004 an die kommunalen Träger und die Agenturen für Arbeit ausgeliefert, um das Erfassen und Bescheiden der Anträge auf Arbeitslosengeld II zu ermöglichen. Dies erforderte auch in Bremen die schnelle Schaffung entsprechender technischer Voraussetzungen, denn bereits zum 1. Januar 2005 sollten die ersten Zahlungen erfolgen. Trotz des Zeitdrucks hat die senatorische Dienststelle sich in den ihr als wesentlich erscheinenden Datenschutzfragen mit mir abgestimmt. Dennoch war das Amt dazu gezwungen, Zugeständnisse zugunsten der Verfahrensfunktionalität zu machen.

Bei dem Programm „A2LL“ handelt es sich um eine internet-basierte Lösung. Es war daher innerhalb einiger Wochen erforderlich, für die ca. 200 Sachbearbeiter/innen der Wirtschaftlichen Hilfe des Amtes für Soziale Dienste einen Internetzugang zu installieren. Da diese parallel einen Zugriff auf das Bremer Sozialhilfeverfahren PROSOZ/PROHEIM von ihren Arbeitsplätzen haben, bestand die Notwendigkeit, das dort bisher erreichte Datenschutzniveau zu halten. Die EDV-Abteilung der senatorischen Dienststelle hat einen Lösungsvorschlag entwickelt, der einen fest installierten ausschließlichen Zugang zu dem Programm „A2LL“ über das Internet ermöglicht. Die entsprechenden Einstellungen sind zentral vorgegeben und an den Arbeitsplätzen nicht veränderbar.

Um den Zugriff von den Arbeitsplätzen auf das Verfahren „A2LL“ über das Internet abzusichern, mussten in Bremen Zertifikate installiert werden. Ein Zertifikat ist eine Sammlung von digital unterzeichneten Daten, die Identitäten von Zertifikatsinhabern garantieren. Das von der Bundesagentur für Arbeit (BA) vorgegebene Verfahren der Zertifikatsbeantragung für die betroffenen Sachbearbeiter/innen wurde in Bremen abgearbeitet. Zur Zertifikatsinstallation gab es von der BA widersprüchliche Anweisungen. In der Installationsanweisung der A2LL-Clientzertifikate für den Internetexplorer wurde als Speicherort für die persönlichen Zertifikate der Sachbearbeiter/innen die lokale Festplatte angegeben. In den Hinweisen zum Umgang mit Softwarezertifikaten für „A2LL“ wurde angeführt, dass die Zertifikate verschlüsselt im Zertifikatsspeicher des Benutzerprofils gespeichert werden.

Die letztgenannte Variante wäre aus Datenschutzsicht die sicherere gewesen. Bremen hat sich aber für die Speicherung auf den lokalen Festplatten entschieden. Die Zertifikate wurden von den Sachbearbeiter/innen selbst installiert. Wesentliche Sicherheitseinstellungen konnten so nicht mehr zentral gesteuert werden. Dazu gehören die Einstellung der Sicherheitsstufe, die Möglichkeit, in einer Checkbox die Einstellung „Kennwort merken“ zu aktivieren (was zu einer Speicherung des Passwortes führt) und die Sicherheitseinstellung für einen zentralen Baustein der Zertifikatssicherheit, der private Schlüssel. Auch wenn davon auszugehen ist, dass die Sachbearbeiter/innen die Installation entsprechend den Sicherheitseinstellungen der Anweisungen vorgenommen haben, ist die aus datenschutzrechtlicher Sicht angemessene technische Steuerung für eine entsprechend sichere Installation nicht erfolgt.

Ein weiteres Problem war die Änderung der Sicherheitsstufe der Zertifikate von „hoch“ nach „niedrig“, die abweichend von den Empfehlungen der BA in Bremen vorgenommen wurde. Sie erfolgte, weil sich bei der vorgesehenen Einstellung „hoch“ die Mitarbeiter auf jeder Seite der Anwendung wieder neu anmelden mussten und ein angemessener Arbeitsfluss damit unterbrochen wurde.

Laut Informationen der senatorischen Dienststelle waren von diesem Problem auch andere Bundesländer betroffen. Die Herunterstufung der Sicherheit aus Gründen der Verfahrensfunktionalität sei der BA bekannt. Sie konnte keine kurzfristige Lösung des Problems anbieten. Die damit verbundene Gefährdung des Datenschutzes kann aus bremischer Sicht allein nicht beurteilt werden. Ich habe daher den Bundesbeauftragten für den Datenschutz (BfD) informiert.

Eine weitere bremische Abweichung von den Hinweisen zum Umgang mit den Softwarezertifikaten war die nicht erfolgte Löschung der durch die BA übergebenen Zertifikatsdateien nach erfolgter Installation. Als Begründung wurde mir der lange Zeitraum genannt (drei bis vier Tage), der von der BA benötigt würde, um ein neues Zertifikat auszustellen. Durch defekte Festplatten seien schon einige Zertifikate verloren gegangen. Vor dem Hintergrund, dass das „A2LL“-System noch nicht unter Volllast arbeitet und in Bremen nur 98 Sachbearbeiter/innen zur gleichen Zeit online sein dürfen (wobei es auch innerhalb dieses Rahmens zu Systemabstürzen kommen soll), sei diese Wartezeit im Hinblick auf die Anforderung, eine Auszahlung des Arbeitslosengeldes ab 1. Januar 2005 gewährleisten zu müssen, unakzeptabel.

Die senatorische Dienststelle stimmte mir über das Erfordernis der Löschung zu, bat aber aus den vorab beschriebenen Gründen darum, die zentrale Speicherung bis zum 31. Januar 2005 zu tolerieren. Ich wies die Dienststelle daraufhin, dass unzulängliche Hardware vor Ort diese Speicherung nicht rechtfertige, habe aber die begrenzte Speicherung unter größtmöglicher technischer und organisatorischer Absicherung aus Gründen der Aufrechterhaltung des Betriebs toleriert.

Die senatorische Dienststelle verfügte über keine Informationen hinsichtlich der Protokollierung der Zugriffe auf die einzelnen Datensätze innerhalb des Verfahrens. Vor dem Hintergrund, dass von jedem Arbeitsplatz auf alle Daten bundesweit lesend zugegriffen werden kann, ist dieser Mangel als gravierender Datenschutzverstoß zu werten. Auch eine Revision ist nicht möglich.

Das durch die BA vorgegebene Berechtigungskonzept ist auf Minimalanforderungen beschränkt.

Die BA hat den Kommunen lediglich Handlungsanweisungen und Umsetzungsempfehlungen zur Verfügung gestellt, jedoch keine Sicherheitskonzeption des Verfahrens. Es war daher in Bremen nicht möglich, die Qualität der einzelnen zu installierenden Sicherheitskomponenten zu bewerten. Weiterführende Fragen zur Verfahrenssicherheit, wie etwa zur Qualität der Verschlüsselung der Datenübertragung oder der Speicherung der für den Zugriff auf „A2LL“ verwendeten Schlüssel blieben auch auf Nachfrage unbeantwortet. Diese Informationslücken, verbunden mit dem enormen Zeitdruck, führten zu den geschilderten datenschutzrechtlichen Problemen und erzwangen förmlich die Priorität der Verfahrensfunktionalität vor einigen Aspekten der Verfahrenssicherheit.

Ich schildere diese vielen verschiedenen Aspekte so ausführlich, weil nur in ihrer Gesamtheit deutlich wird, wie letztendlich bei der Einführung eine Gefährdung des Datenschutzes von der BA billigend in

Kauf genommen wurde. Die Stellen im Land Bremen trifft insofern keine Schuld. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die gravierenden technischen Mängel in einer einstimmig gefassten Entschließung (vgl. Ziff. 15.8 dieses Berichts) aufgeführt.

10. Bildung und Wissenschaft

10.1 Prüfung der Schüleraktenführung in einer Privatschule

In der Freien Evangelischen Bekenntnisschule Bremen (FEBB) habe ich eine Prüfung der Schüleraktenführung durchgeführt. Die Schule hat erklärt, sie orientiere sich bei der Aktenhaltung an den Vorgaben des Gesetzes zum Datenschutz im Schulwesen (BremSchulDSG).

- Unterlagen mit sensiblen Daten in der Schullaufbahnakte

  Die Schullaufbahnakten unterteilen sich in die Teile A und B. Während in Teil A Zeugnisse aufgenommen werden, enthält Teil B alle weiteren Unterlagen (z. B. den Förderbedarf, Lernschwächen, Behinderungen oder Krankheiten betreffend). In einer Stichprobe habe ich durch Einsichtnahme mehrere Akten einer Datenschutzprüfung unterzogen.

  In einer eingesehenen Schullaufbahnakte befanden sich zahlreiche Unterlagen mit sehr sensiblen Daten, die u. a. die Behinderung eines Schülers betreffen. Da nicht alle diese Unterlagen zur Erfüllung des Unterrichts- und Erziehungsauftrags benötigt wurden, habe ich gebeten, den Akteninhalt auf seine Notwendigkeit hin zu überprüfen und nicht benötigte Unterlagen den Erziehungsberechtigten des Schülers auszuhändigen oder datenschutzgerecht zu vernichten. Andere Akten mit vergleichbarem Inhalt will die Schule prüfen. Auch habe ich empfohlen, die für die Aufnahme von Unterlagen in Teil B der Schullaufbahnakte erforderlichen schriftlichen Einwilligungserklärungen der Erziehungsberechtigten in die Akten mit aufzunehmen, da diese fehlten.

- Vernichtung von Schullaufbahnakten

  Die Vertreter der FEBB teilten mit, dass eine Aussonderung von Akten ehemaliger Schüler bislang nicht erfolgt sei. Ihnen fehlten hierzu insbesondere Regelungen, wie sie bei der Aussonderung vorgehen sollen.

  Ich habe empfohlen, die Vorschriften des § 18 BremSchulDSG und die Richtlinien über die Sicherung, Aufbewahrung und Aussonderung von Schriftgut in den Schulen des Senators für Bildung und Wissenschaft entsprechend anzuwenden. Danach sind Schullaufbahnakten grundsätzlich nicht länger als drei Jahre nach Ende der Schulzeit aufzubewahren. Nach Ablauf dieser Frist sind die Akten auszusondern und einer datenschutzgerechten Vernichtung zuzuführen. Daneben gelten besondere Aufbewahrungsfristen insbesondere für Zweitschriften von Abschluss-, Abgangs- und Prüfungszeugnissen. Außerdem habe ich jährliche Löschungsroutinen empfohlen. Die Schule hat zugesagt, meine Empfehlungen umzusetzen.

Als wesentliches Ergebnis ließ sich festhalten, dass die Führung der Schülerakten in dieser Privatschule überwiegend den Datenschutzanforderungen entspricht.

10.2 Forschungsprojekte und andere Untersuchungen an Schulen

Auch im Berichtszeitraum sind verschiedene Forschungsprojekte und andere Untersuchungen an Schulen durchgeführt worden, zu denen ich Stellungnahmen abgegeben habe. Vor der Durchführung eines solchen Projekts bin ich neben dem Elternbeirat und dem Schülerbeirat nach § 13 Abs. 6 Gesetz zum Datenschutz im Schulwesen (BremSchulDSG) zu unterrichten. Dies bedeutet, dass ich nur bei rechtzeitiger Unterrichtung in der Lage bin, auf eine datenschutzkonforme Gestaltung der Vorhaben hinzuwirken. Leider wurde ich nicht selten erst bei oder unmittelbar vor Beginn des Projektes unterrichtet, was gelegentlich dazu geführt hat, dass meine Vorschläge zur Verbesserung des Datenschutzes nicht mehr umgesetzt werden konnten. Zwei interessante Forschungsvorhaben stelle ich nachstehend vor:

- Sprachcamp in den Sommerferien

  Das Sprachsommercamp wurde vom Senator für Bildung und Wissenschaft unter wissenschaftlicher Begleitung des Max-Planck-Instituts Berlin durchgeführt. Eine Gruppe von Schulkindern der dritten Klasse, die aktiv am Sommercamp teilnahm, sollte eine intensive Sprachförderung erhalten. Vorher wurde von den Teilnehmern und deren Eltern mit Hilfe von Fragebogen erhoben, unter welchen Bedingungen die Kinder leben und lernen.

  Für eine solche intensive Datenerhebung ist eine wirksame Einwilligung erforderlich. Voraussetzung hierfür ist eine angemessene Unterrichtung. Ich habe deshalb vorgeschlagen, den Eltern vor Beginn des Sommercamps neben der Übersendung des vorgesehenen Informationsblatts und der Einwilligungserklärung auch zu ermöglichen, den Schüler- und Elternfragebogen einzusehen.

  Geplant war auch, mit Hilfe von Bildgeschichten und anderen Gesprächssituationen Sprachproben von den Schulkindern auf Video aufzuzeichnen. Dabei sollten die “schönsten Aufnahmen“ der Schule zur Verfügung gestellt werden. Zwar werden die Eltern über den Zweck und die weitere Verwendung der Videoaufnahmen informiert. Es ist jedoch nicht auszuschließen, dass durch die Videoaufnahmen evtl. Sprachfehler, -mängel oder sonstige Beeinträchtigungen der Schüler festgehalten werden. Zur Wahrung der schutzwürdigen Interessen der betroffenen Schulkinder und Eltern habe ich daher empfohlen, ihnen Gelegenheit zu geben, die Videoaufzeichnung ihres Kindes vor der Weitergabe der „schönsten Aufnahmen“ an die Schule einzusehen, damit sie dann entscheiden können, ob sie einer Weitergabe zustimmen.

  Der Senator für Bildung und Wissenschaft hat das Max-Planck-Institut gebeten, meine Vorschläge zu berücksichtigen.

- Wissenschaftliche Begleitung des Programms „Schule macht sich stark“

  Im Rahmen einer begleitenden Studie sollten die Möglichkeiten zur Verbesserung von Unterricht und Schulleben wissenschaftlich untersucht werden. Hierzu sollten mit einem Fragebogen die Lebens- und Lernbedingungen der Schülerinnen und Schüler innerhalb und außerhalb der Schule erhoben werden. Mit Hilfe eines Elternbriefs sollten die Erziehungsberechtigten darüber informiert

und um Einwilligung zur Teilnahme ihrer Kinder an der wissenschaftlichen Begleitung gebeten werden. Mir wurden nur wenige Tage Frist gegeben, um zu dem Vorhaben Stellung zu nehmen.

Da die Fragen auch Angaben über die ethnische Herkunft der Eltern und Kinder sowie Angaben über die politische Meinung der Kinder zu bestimmten Themen betreffen, habe ich dargelegt, dass sich die Einwilligung der Erziehungsberechtigten gem. § 3 Abs. 2 Nr. 2 Bremisches Datenschutzgesetz (BremDSG) ausdrücklich auf diese besonderen Arten von Daten beziehen muss, so dass sowohl der Elternbrief als auch die Einwilligungsklausel entsprechend hätten geändert werden müssen. Bevor ich in dieser Weise dem Senator für Bildung und Wissenschaft meine Vorschläge unterbreiten konnte, hatte ich bereits Beschwerden von Eltern bekommen, die über den Elternbrief verfügten.

Ich habe daher gegenüber der senatorischen Dienststelle moniert, dass ich nicht vor, sondern erst nach Beginn über das wissenschaftliche Vorhaben unterrichtet worden bin.

Konsequenz meiner verspäteten Beteiligung war, dass der nach meinen Vorschlägen überarbeitete Elternbrief und die ergänzende Einwilligungserklärung ein zweites Mal an die Erziehungsberechtigten versandt werden mussten, weil die Einwilligung der Eltern wegen der Nichtbeachtung der Anforderung bei der Erhebung besonderer Arten von Daten nicht wirksam gewesen wäre.

Darüber hinaus haben Eltern mir gegenüber erklärt, in einer Schule hätten ihre Kinder trotz der nicht erteilten Einverständniserklärung der Erziehungsberechtigten an der Fragebogenaktion teilnehmen müssen. Auf meine Anfrage hat die Schulleitung dieser Schule erklärt, bei einer Befragung der Lehrerinnen und Lehrer hätte sich herausgestellt, dass nicht bei allen Schülerinnen und Schüler auf die Vorlage der Einwilligungserklärung geachtet worden sei und bei einer erneuten Fragebogenaktion würde verstärkt darauf geachtet werden, dass Kinder bei Ablehnung der Einwilligung durch die Eltern nicht an der Erhebung teilnehmen werden.

Zwischenzeitlich hat sich der Rechtsausschuss mit der Problematik der verspäteten Beteiligung meiner Dienststelle beschäftigt und mich in meiner Auffassung einer rechtzeitigen Unterrichtung unterstützt. Ein Vertreter des Senators für Bildung und Wissenschaft zeigte zwar auf, wie kurz oft die Umsetzungsfristen solcher Projekte sind, sagte aber zu, in Zukunft darauf zu achten, mich frühzeitig zu beteiligen.

10.3 Arbeitsentwurf zur Novellierung des bremischen Schuldatenschutzgesetzes

Seit dem In-Kraft-Treten des bremischen Schuldatenschutzgesetzes (BremSchulDSG) im Jahre 1987 ist aufgrund der praktischen Erfahrungen mit diesem Gesetz, der EU-Datenschutz-Richtlinie aus dem Jahre 1995, der daraufhin erfolgten Novellierung des Bremischen Datenschutzgesetzes (BremDSG) im Jahre 2002 und der Weiterentwicklung der automatisierten Datenverarbeitung auch im Schulbereich eine Novellierung des BremSchulDSG geboten.

Aus diesem Grunde haben bereits mehrere Besprechungen mit Vertretern des Senators für Bildung und Wissenschaft stattgefunden, in denen im Wesentlichen zu folgenden Punkten Einvernehmen hergestellt worden ist:

- Datenverarbeitung durch Lehrkräfte außerhalb der Schule

  Nach geltendem Recht dürfen sog. „Schulbedienstete“ Schülerdaten weder auf privateigenen Datenverarbeitungsgeräten noch auf Datenverarbeitungsgeräten außerhalb der Schule (also am häuslichen Arbeitsplatz) verarbeiten. Nunmehr soll praxis- und datenschutzgerecht geregelt werden, dass Lehrkräfte zur Erfüllung ihrer Aufgaben Schülerdaten auch in ihrer privaten Umgebung verarbeiten dürfen. Voraussetzung ist jedoch, dass sie sich schriftlich zur Beachtung der datenschutzrechtlichen Vorschriften verpflichten und mit der Überwachung durch den behördlichen Datenschutzbeauftragten und den Landesbeauftragten für den Datenschutz einverstanden erklärt haben. Diese Regelung entspricht weitgehend den Anforderungen, die auch bei der sog. „Alternierenden Telearbeit“ einzuhalten sind (vgl. Ziff. 5.3 dieses Berichts).

- Automatisierte Verarbeitung von Schülerdaten

  Bei der Schaffung des BremSchulDSG im Jahre 1987 befand sich die automatisierte Datenverarbeitung noch in den „Kinderschuhen“, so dass seinerzeit - durchaus praxisgerecht - detailliert festgelegt wurde, welche personenbezogenen Schülerdaten automatisiert bzw. nicht automatisiert verarbeitet werden dürfen. Aufgrund der rasanten Entwicklung, insbesondere zum heute nicht mehr wegzudenkenden PC-Arbeitsplatz und dem im Schulbereich verwendeten Verarbeitungsprogramm MAGELLAN, ist diese Differenzierung unrealistisch, so dass sie bei der Novellierung grundsätzlich aufgehoben werden soll.

- Datenverarbeitungsregelung im Gesetz und Datenkatalog per Rechtsverordnung

  Vorgesehen ist nunmehr, im BremSchulDSG nur noch materiell-rechtlich zu regeln, zu welchen Zwecken Schulen Daten über Schülerinnen und Schüler verarbeiten dürfen und den Umfang der zu den jeweiligen Zwecken zu verarbeitenden Daten auf der Grundlage einer gesetzlichen Ermächtigungsnorm in einer Rechtsverordnung festzulegen. Dies ist aus Sicht des Bildungsressorts insbesondere deshalb notwendig, weil dadurch nicht mehr bei jeder Erweiterung des jeweiligen Datenkatalogs die Gesetzgebung bemüht werden muss.

- Einbeziehung der Privatschulen

Da das Persönlichkeitsrecht der Schülerinnen und Schüler bei der Datenverarbeitung sowohl durch öffentliche Schulen als auch durch private sowie anerkannte Ersatzschulen in gleicher Weise tangiert ist, sollen diese Schulen – soweit sie allgemeinbildende oder berufliche Schulen sind – in den Geltungsbereich dieses Gesetzes aufgenommen werden.

- Untersuchungen und wissenschaftliche Forschung

  Grundsätzlich ist bei allen Untersuchungen und wissenschaftlichen Forschungsvorhaben (z. B. Pisa-Studie; vgl. 26. JB, Ziff. 10.1.1) die Einwilligung der Schülerinnen und Schüler und – abhängig vom jeweiligen Alter bzw. Reifegrad dieses Personenkreises – der Erziehungsberechtigten erforderlich. Aufgrund neuerer technischer Entwicklungen auf dem Gebiet der Pseudonymisierung soll auf die Einwilligung verzichtet werden, wenn der Zweck der entsprechenden Untersuchung durch Verwendung pseudonymisierter Daten erreicht werden kann. Voraussetzung soll dabei sein, dass

  - die Nutzung der Schülerdaten ausschließlich durch Verwendung einer zweiten Datenbank, die nur pseudonymisierte Daten enthält, erfolgt,
  - das Pseudonym so gestaltet wird, dass ein Bezug zu Datensätzen der zweiten Datenbank herstellbar, die Identifikation einer Person aber ausgeschlossen ist und
  - die Ergebnisse der pseudonymisierten Untersuchungen keine Einzelmerkmale enthalten, die einen Rückschluss auf die Identität einzelner Schüler zulässt.

Inzwischen hat das Bildungsressort einen Arbeitsentwurf erarbeitet, der die vorgenannten Punkte und eine Vielzahl anderer Korrekturen enthält. Vereinbart worden ist, dass zunächst eine schulinterne Abstimmung erfolgt. Ich denke, dass die bisher konstruktive Kooperation mit dem Bildungsressort zu einer insgesamt praxis- aber auch datenschutzkonformen Weiterentwicklung des Datenschutzes in den Schulen beitragen wird.

11. Bau, Wirtschaft und Häfen

11.1 Durchführungsverordnung zum Landesvergabegesetz

Das Vergabegesetz des Landes Bremen (Brem.GBl. 2002, S. 594) enthält in § 9 Abs. 4 Satz 1 eine Befugnis des Senats, ein Register über Unternehmen einzurichten, die gegen Verpflichtungen dieses Gesetzes verstoßen (Tariftreuepflicht). In dieses Register eingetragene Unternehmen können für die Dauer von bis zu zwei Jahren von der öffentlichen Vergabe von Aufträgen ausgeschlossen werden.

Die darauf fußende und mit mir abgestimmte Verordnung nach § 9 Abs. 2 Satz 2 zur Durchführung des Vergabegesetzes (VergV) vom 21. September 2004 (Brem.GBl. 2004, S. 475) enthält normenklare Regelungen u. a. über

- die im Register zu speichernden Daten, den Zeitpunkt ihrer Löschung und die Einsichtnahme in das Register,
- die Verpflichtung der öffentlichen Auftraggeber (Vergabestellen), Entscheidungen über Verstöße gegen dieses Gesetz an das Register zu melden und
- die Verpflichtung der öffentlichen Auftraggeber, zur Prüfung der Zuverlässigkeit von Unternehmen Auskünfte aus dem Register einzuholen.

11.2 Hafensicherheit

Nach dem Terroranschlag in den USA vom 11. September 2001 wurde das SOLAS-Abkommen dahingehend geändert, dass nunmehr ein unkontrollierter und ungesteuerter Zugang zu den Hafenanlagen nicht mehr möglich sein soll. Bei den Planungen für die verstärkten Sicherheitsmaßnahmen in den Häfen wurde ich beteiligt (vgl. 26. JB, Ziff. 12.2). Im Juli 2004 sind das Gesetz zur Ausführung der Änderungen des Internationalen Übereinkommens von 1974 zum Schutz des menschlichen Lebens auf See und des Internationalen Codes für die Gefahrenabwehr auf Schiffen und in den Hafenanlagen vom 25. Juni 2004 (BGBI. I 1389), für dessen Namen ich nicht verantwortlich bin, und das bremische Hafensicherheitsgesetz vom 6. Juli 2004 (Brem.GBI. S. 405) in Kraft getreten. Durch diese gesetzlichen Vorschriften sind im Lande Bremen zur Zeit 67 Hafenanlagenbetreiber verpflichtet, die in den Gefahrenabwehrplänen festgelegten Sicherheitsauflagen zu erfüllen und entsprechende Sicherheitsmaßnahmen zu treffen.

Ich habe exemplarisch bei drei großen bremischen Hafenanlagenbetreibern eine Datenschutzprüfung vorgenommen. Das Betreten bzw. Befahren des Geländes ist nur mit einer entsprechenden Erlaubnis gestattet. In allen drei Betrieben wurden ähnliche Verfahren zur Erlangung einer Erlaubnis z. B. in Form einer Tagesausnahmegenehmigung (Tagesausweis/Besucherausweis) oder einer Dauerausnahmegenehmigung (Dauerausweis) eingeführt. Dabei findet in jedem Fall eine Prüfung der Identität, ein Bildvergleich und die Aufnahme der Ausweisdaten statt. Das Betreten und Verlassen des Geländes wird über entsprechende technische Anlagen festgehalten. Aus dem Bereich der Betroffenen, die häufig Transportgut in den Hafenanlagen abliefern oder abholen müssen (insbesondere Trucker) oder dort bestimmte Tätigkeiten verrichten müssen (Handwerker), habe ich eine Reihe von Eingaben erhalten, die sich gegen die - aus ihrer Sicht - überzogenen Sicherheitsmaßnahmen richteten. Ich wurde gebeten zu prüfen, was mit den Daten im Einzelnen geschieht. Einige Eingaben richteten sich gegen das Verfahren vor der Ausstellung von Tagesausweisen und gegen unterschiedliche Maßstäbe im Vergleich zu den Sicherheitsmaßnahmen in den Häfen anderer Länder. Während ich die Verfahrensmängel abstellen konnte, kann ich zu den unterschiedlichen Umsetzungsständen der Sicherheitsmaßnahmen in den verschiedenen Ländern der EU keine Bewertung vornehmen.

Bei Ein- und Ausfahrten in das bzw. aus dem Hafengebiet findet eine Überwachung durch Videoanlagen und eine Speicherung der Bilddaten statt. Je nachdem, in welchem Bereich (z. B. Fußgänger-Drehkreuze, Kfz-Schleusen, Einfahrt für Lkw mit Container) die Videoüberwachung stattfindet, werden Aufnahmen von Personen, Kraftfahrzeugen einschließlich Kennzeichen sowie Containertransportern mit Datumsangaben aufgezeichnet. Es fehlt allerdings ein Hinweis auf die Videoüberwachung und die Nennung der verantwortlichen Stelle, so wie es der § 6 b des Bundesdatenschutzgesetzes (BDSG) vorschreibt. Hierauf habe ich hingewiesen.

Derzeit prüfe ich die Verfahrensbeschreibungen der Hafenanlagenbetreiber. Mit dieser Prüfung beabsichtige ich, die Zweckbindung der Daten und die Beachtung des Grundsatzes der

Datensparsamkeit sicherzustellen sowie zu erreichen, dass die Daten so früh wie rechtlich möglich gelöscht werden.

Parallel dazu berate ich die Regelung des Verfahrens der Zuverlässigkeitsprüfung nach dem Hafensicherheitsgesetz. Diese Verordnung ist erforderlich, um die Sicherheitsüberprüfung der Personen in den Hafenanlagen zu regeln, die mit der Gefahrenabwehr direkt beauftragt sind.

Der übersandte Entwurf entsprach in weiten Teilen nicht den gesetzlichen Vorgaben aus § 13 des Hafensicherheitsgesetzes. Insbesondere sieht er Datenübermittlungen zwischen der für die Zuverlässigkeitsüberprüfung zuständigen Stelle und den Arbeitgebern der zu überprüfenden Personen vor, also genau das, was mit dem Gesetz verhindert werden sollte. Hierauf habe ich in meiner Stellungnahme hingewiesen und erwarte einen neuen Entwurf.

12. Finanzen

12.1 Steuerehrlichkeit – aber mit Datenschutz

Mit dem Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003 (BGBl. I 2003, S. 2928) wird den Finanzbehörden und anderen Behörden die Möglichkeit eingeräumt, über das Bundesamt für Finanzen bei den Kreditinstituten in der Bundesrepublik Deutschland die personenbezogenen Daten von Inhabern, Verfügungsberechtigten und sonstigen mit einem Konto wirtschaftlich verbundenen Personen abzurufen. Diese Regelung gewährt den Finanzbehörden das Recht, gezielte Ausforschungen zu Konten und Depots zu betreiben. Damit erhalten die Finanzbehörden zwar unmittelbar keine Kenntnis von den Kontenständen und den näheren Umständen, etwa den Umfang der Verfügung oder Bewirtschaftung; allerdings kann die Finanzbehörde im Rahmen des Besteuerungsverfahrens nun gezielt den Steuerbürger danach befragen und, wenn ihr die Auskünfte nicht ausreichen, auch das betreffende Kreditinstitut gemäß § 93 Abgabenordnung (AO) direkt und umfassend um Auskunft ersuchen. Damit steht den Finanzbehörden erstmalig ein totales Überwachungssystem zur Verfügung, das auch die nicht steuerpflichtigen Bürger einschließt.

Alle Personen, die bei deutschen Kreditinstituten Konten oder Depots unterhalten, für die sie verfügungsberechtigt oder wirtschaftlich verantwortlich sind, sind für die Finanzbehörden gläsern. Jede Konto- oder Depoteröffnung wird für die Finanzbehörde nachvollziehbar.

Doch nicht nur die Finanzbehörden sollen diese Informationserhebungsrechte erhalten, sondern auch andere öffentliche Stellen. Welche das sind, wird im Gesetz nicht konkret festgelegt. Die gesetzliche Festlegung besteht lediglich darin, dass die anfordernde Behörde bei der Gewährung von Leistungen das Einkommensteuerrecht anwendet, die Auskünfte von dem Betroffenen nicht zu erhalten sind und ihre Aufgabenerfüllung ohne die Kenntnis gefährdet wäre. Diese Regelung ist zu vage, denn für die Bürger ist nicht absehbar, in welchen Fällen sie betroffen sind und wann von der Regelung Gebrauch gemacht wird. Ohne ergänzende gesetzliche Regelungen, etwa in den bereichsspezifischen Anwendungsfällen, begegnet diese Regelung verfassungsrechtlichen Bedenken. In jedem Fall muss der Betroffene über den Abruf informiert werden.

Es muss gesetzliche Festlegungen geben, welche Behörden die Informationen abrufen dürfen. Weiter ist sicherzustellen, dass die Finanzbehörden die Daten, die ihnen im Wege der Amtshilfe dabei zur Kenntnis gelangen, nicht selbst verwenden dürfen.

Die Regelungen der AO treten am 1. April 2005 in Kraft. Betroffene haben Verfassungsbeschwerde gegen die genannten gesetzlichen Regelungen eingelegt. Die Datenschutzbeauftragten des Bundes und der Länder haben in ihrer Entschließung “Staatliche Kontenkontrolle muss auf den Prüfstand!“ Bedenken erhoben (vgl. Ziff. 15.10 dieses Berichts).

12.2 Steuererklärungen über das Internet

Um festzustellen, in welchem Umfang Bremer Bürger von der Möglichkeit einer elektronischen Steuererklärung Gebrauch machen, habe ich mich bei den Finanzbehörden erkundigt. Nach deren Mitteilung hat die Zahl der Steuererklärungen stark zugenommen. So sind bis zum September 2004 circa 21.000 Einkommensteuererklärungen über das Internet eingegangen, im Jahr 2003 waren es noch 4.135.

Es ist damit zu rechnen, dass die Zahl im nächsten Jahr weiter erheblich ansteigen wird, weil den Steuerpflichtigen in den meisten Fällen nicht mehr die Lohnsteuerkarte ausgehändigt wird und die Einkommensdaten vom Arbeitgeber in elektronischer Form unmittelbar an das Finanzamt geliefert werden. Hinzu kommt, dass in vielen Fällen eine so genannte Vereinfachte Steuererklärung abgegeben werden kann.

Ich berate die Steuerbürger dahingehend, die Sicherheitsvorkehrungen, die die Anwendung ELSTER (elektronische Steuererklärung) bietet, vollständig zu nutzen und unterstütze die Einhaltung der Sicherheitsmaßnahmen in den Finanzbehörden Bremens durch aktive Beteiligung an der Fortentwicklung des Datenschutzkonzeptes.

13. Bremerhaven

Da es sich anbietet, viele Themen in einem Sachzusammenhang darzustellen, soll an dieser Stelle die Auffindbarkeit von Beiträgen erleichtert werden, die Themen aus Bremerhaven betreffen. Sie finden sich unter Ziff. 1.4 (Behördliche Datenschutzbeauftragte), Ziff. 1.8 (Gravierende Datenschutzmängel beim Arbeitslosengeld II), Ziff. 1.11 (Droht der genetisch gläserne Mensch?), Ziff. 3.3.2 (Funk-LAN-Prüfung im Helene-Kaisen-Haus), Ziff. 4.1 (Ergebnisse der Beratung des 26. Jahresberichts), Ziff. 4.2 (Weitere Themen der Beratungen im Rechtsausschuss), Ziff. 5.2 (Ein Leserbrief mit Folgen), Ziff. 6.1 (Prüfungen vom Polizeirevieren), Ziff. 6.3 (DNA-Reihenuntersuchung), Ziff. 6.5 (Automatisches Fingerabdruck-System), Ziff. 6.8 (Sicherheitsmaßnahmen bei Verlust der Kredit- oder EC-Karte), Ziff. 6.11 (Bürgerbüro Bremerhaven), Ziff. 9.1 (Datenerhebung für das Arbeitslosengeld II).

14. Datenschutz in der Privatwirtschaft

14.1 Prüfung der Datensicherheit in Bremer Arztpraxen

Innerhalb von Arztpraxen gibt es viele sensible Bereiche, in denen Patientendaten verarbeitet werden. Hierzu gehören beispielsweise der Empfang, der Behandlungsbereich, die Praxisverwaltung und die EDV.

Ich habe in diesem Jahr die Verarbeitung der Patientendaten und deren Schutz in den EDV-Netzen einzelner Praxen geprüft.

Dabei konnte ich feststellen, dass entgegen meinen Erwartungen keine Zugänge aus den Praxisnetzen in das Internet vorhanden waren. Dies hätte hohe Schutzmaßnahmen zur Abgrenzung der Praxisnetze gegenüber dem öffentlichen Netz erfordert. Schutzmaßnahmen wären beispielsweise der Einsatz der Firewalltechnologie und/oder der Aufbau speziell geschützter Kommunikationsstrecken gewesen.

Weiterhin konnte ich feststellen, dass auch direkte E-Mail-Verbindungen in und aus den Praxisnetzen nicht vorhanden waren. Damit mussten keine Schutzmaßnahmen gegenüber dem Eindringen von Schadsoftware (Viren, Würmern, Trojaner etc.) in das Praxisnetz ergriffen werden.

Ein elektronischer Datenaustausch fand lediglich zu Abrechnungszwecken per Diskette in verschlüsselter Form statt.

Ich fand lokale Praxisnetze vor, die die Sicherheitsmaßnahmen der zu Grunde liegenden Netzbetriebssysteme zur Implementierung von Datensicherungsmaßnahmen nutzten. Dazu gehörten eine datenschutzgerechte Zugriffssteuerung auf die Patientendaten über die Möglichkeiten der Benutzerverwaltung und die Vergabe von Datei- und Verzeichnisrechten. Darüber hinaus wurden die Authentifizierungsmechanismen der Betriebssysteme als Grundlage für den vertraulichen Zugriff auf die Daten genutzt. Auf der Anwendungsebene (innerhalb der Praxissoftware) wurden ebenfalls Zugriffssteuerungsmechanismen eingesetzt. Insgesamt konnte ich feststellen, dass bei den geprüften Stellen innerhalb der Praxisnetze auf der Grundlage der eingesetzten Softwareprodukte angemessene Datenschutzmaßnahmen ergriffen worden sind.

14.2 Prüfung eines Marktforschungsinstituts

Unter Zugrundelegung der Registermeldung des Unternehmens nach § 4 d Bundesdatenschutzgesetz (BDSG) befasste ich mich im Berichtsjahr mit der Datenverarbeitung eines Bremer Marktforschungsinstituts. Das Institut hat es sich u. a. zur Aufgabe gemacht, für Kunden bevölkerungsrepräsentative Erhebungen auf Stichprobenbasis durchzuführen. Wie mir vom Institut weiter mitgeteilt wurde, werden von ihm für die Durchführung dieser Erhebungen personenbezogene Daten verarbeitet, jedoch nicht an den jeweiligen Auftraggeber weitergegeben; diese erhalten von ihm nur Ergebnisse, die keinen Bezug zu den antwortenden Personen mehr zulassen (Repräsentativergebnisse mit aggregierten Daten).

Das Institut hatte es unterlassen, einen betrieblichen Datenschutzbeauftragten zu bestellen. Eine Notwendigkeit zu einer Bestellung hatte das Unternehmen mit dem Hinweis auf die geringe Anzahl festangestellter Mitarbeiter bislang nicht gesehen. Dabei wäre das Unternehmen schon seit längerer Zeit zur Bestellung eines betrieblichen Datenschutzbeauftragten verpflichtet gewesen. Gem. § 4 f Abs. 1 Satz 5 BDSG haben nicht öffentliche Stellen, die personenbezogene Daten geschäftsmäßig zum Zweck der anonymisierten Übermittlung erheben, verarbeiten oder nutzen, unabhängig von der Zahl der Arbeitnehmer einen Beauftragten für den Datenschutz zu bestellen. Unter diese Regelung fiel im vorliegenden Fall auch das Marktforschungsinstitut. Auf meine Kritik hin wurde schließlich ein betrieblicher Datenschutzbeauftragter bestellt.

Sehr unzureichend waren auch die vom Marktforschungsinstitut in seiner Registermeldung zu § 4 d Satz 1 Nr. 9 BDSG gemachten Angaben, die eine allgemeine Beschreibung der getroffenen technischen und organisatorischen Sicherungsmaßnahmen geben sollen. Insbesondere fehlten Angaben hinsichtlich der eingesetzten Hard- und Software, der Vernetzung des Instituts sowie der ergriffenen Sicherungsmaßnahmen. Eine Beurteilung der Datensicherheit bei dem Institut war deswegen unmöglich. Auf meine Anforderung hin wurden mir von dem Unternehmen die notwendigen Unterlagen zur Verfügung gestellt und die nach § 4 d BDSG erforderliche Ergänzung der Registermeldung von ihm vorgenommen.

14.3 Aus Angst wollen Arbeitnehmer bei Beschwerden anonym bleiben

Im Berichtszeitraum hat sich die Anzahl der Beschwerden im Bereich des Arbeitnehmerdatenschutzes nicht wesentlich verändert. Dagegen habe ich kaum noch schriftliche, dafür umso mehr telefonische Eingaben bzw. Anfragen erhalten. Hierbei ist besonders auffällig, dass die Anrufer häufiger als sonst ihren Namen selbst am Telefon nicht sagen möchten, weil sie völlig anonym über ihre Datenschutzrechte im Arbeitsverhältnis informiert und besonders zu konkreten Problemen beraten werden möchten.

Auf die gelegentliche Nachfrage nach dieser besonderen Zurückhaltung erklären die Anrufer, sie hätten Angst um ihren Arbeitsplatz und wüssten nicht, ob die Gespräche vom Arbeitgeber mitgehört werden könnten. Mein regelmäßiges Angebot, beim Arbeitgeber - selbstverständlich ohne Namensnennung des Anrufers - nachzufragen oder gar zu prüfen, wird fast immer abgelehnt. Wenn sich jemand „traut“ und seinen Arbeitgeber beim Namen nennt, wird häufig darum gebeten, erst mehrere Wochen oder gar Monate nach dem Anruf beim Arbeitgeber vorstellig zu werden.

Ich halte diese Situation für äußerst problematisch. Gerade nach der Novellierung des Bundesdatenschutzgesetzes (BDSG) im Jahr 2001 sind die Rechte der Betroffenen erheblich verbessert worden. Insbesondere regelt § 38 i. V. m. § 21 BDSG, dass sich jedermann an die Aufsichtsbehörde für den Datenschutz wenden kann, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten in seinen Rechten verletzt worden zu sein. Auch wenn in dieser Vorschrift im Gegensatz zu den meisten Landesdatenschutzgesetzen kein ausdrückliches Benachteiligungsverbot enthalten ist, meine ich, dass auch im nicht öffentlichen Bereich niemand benachteiligt werden darf, wenn er sich wegen der Verletzung seiner Datenschutzrechte an die Aufsichtsbehörde für den Datenschutz wendet.

Insgesamt behandelten die Anfragen häufig Zweifel, ob und in welchem Umfang der Arbeitgeber die Internet- und E-Mail-Nutzung am Arbeitsplatz überwachen darf. Anrufer berichteten auch darüber, sie hätten Bewerbungsunterlagen anderer abgewiesener Bewerber erhalten.

14.4 Verarbeitung von Leih- und Zeitarbeitnehmerdaten

Im Berichtsjahr habe ich die Erhebung und Speicherung von Arbeitnehmerdaten bei drei Firmen geprüft, deren Geschäftsfelder die Arbeitnehmerüberlassung für gewerbliche und kaufmännische Arbeiten in anderen Betrieben und die Personalvermittlung sind. Die Betroffenen sind regelmäßig Beschäftigte dieser Firmen und werden zeitlich befristet für bestimmte Tätigkeiten oder für ein bestimmtes Projekt anderen Firmen („Kunden“) überlassen. Vor der Aufnahme in die Vermittlung bzw. in das Beschäftigungsverhältnis bei einer der überprüften Firmen müssen die Arbeitswilligen einen Personalfragebogen ausfüllen, der im Wesentlichen Fragen nach Fähigkeiten und Einsatzmöglichkeiten bzw. -einschränkungen, insbesondere aus familiären Gründen, beinhaltet.

Umfang der Datenerhebung: Ich habe mir die Personalfragebogen der Firmen jeweils vorlegen lassen und geprüft. Die Erhebung der darin vorgesehenen Daten ist nur zulässig, soweit sie für das einzugehende Beschäftigungsverhältnis erforderlich ist (§ 28 Abs. 1 Nr. 1 Bundesdatenschutzgesetz – BDSG). Hierbei sind die ständige Rechtsprechung des Bundesarbeitsgerichts und des Europäischen Gerichtshofs zu berücksichtigen, wonach sich das Fragerecht des Arbeitgebers nur auf die zu besetzende Stelle erstreckt und die Auskunftspflicht des Bewerbers dort aufhört, wo sein Persönlichkeitsrecht tangiert wird, ohne dass hierfür sachliche Gründe vorliegen.

Darüber hinaus ist die Erhebung von Angaben, die vermeintlich auf freiwilliger Basis erfragt werden, in der Regel nicht zulässig, weil sie gerade im Bewerbungs- bzw. Arbeitsverhältnis regelmäßig nicht auf der freien Entscheidung des Betroffenen beruht, so dass die Voraussetzungen des § 4 a BDSG nicht vorliegen.

Unter diesen Prämissen ist die Zulässigkeit der Erhebung folgender Daten in den Personalfragebogen mit den Firmen erörtert worden:

Daten zum Lohn bzw. Gehalt beim letzten Arbeitgeber: In einem der geprüften Unternehmen werden diese Angaben erhoben. Sie seien erforderlich, weil in der Branche mehrere Tarifverträge für Zeitarbeit existierten, die jeweils andere Firmen mit jeweils anderen Gewerkschaften abgeschlossen haben. Die Daten zum Stundenlohn bzw. Gehalt beim letzten Arbeitgeber seien zur Durchführung des Bewerbungsverfahrens hilfreich. Auf Nachfrage wurde eingeräumt, alle Beschäftigten würden weitestgehend gleich bezahlt.

Insoweit ist die Erhebung von Angaben zum letzten Lohn bzw. Gehalt nicht erforderlich und demzufolge unzulässig.

Mitglied eines Berufsfachverbandes: Ebenfalls in nur einer der geprüften Firmen wurde diese Angabe erhoben mit der Begründung, es wäre interessant zu wissen, ob ein Bewerber z. B. im Verband Deutscher Ingenieure (VDI) ist.

Da zu den Berufsfachverbänden auch die Gewerkschaften gehören, ist die Erhebung dieses Datums insbesondere deshalb unzulässig, weil es sich bei Angaben über die Gewerkschaftszugehörigkeit um besondere Arten von Daten nach § 3 Abs. 9 BDSG handelt. Sie dürfen nur unter den Voraussetzungen des § 28 Abs. 6 bis 9 BDSG verarbeitet werden, u. a. nur mit Einwilligung der

Betroffenen oder durch Organisationen, die gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, soweit dies für die Tätigkeit der Organisation erforderlich ist. Dies gilt nur für personenbezogene Daten der Mitglieder oder der Organisation von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten.

Weil diese Voraussetzungen im Prüffall nicht vorlagen, ist von der Firma erklärt worden, auf die Erhebung dieser Angaben werde nunmehr verzichtet.

Angaben über Schwerbehinderung: Angaben hierzu wurden im Bewerbungsverfahren von zwei der geprüften Unternehmen erhoben. Die Erforderlichkeit wurde u. a. mit der Schwerbehindertenquote begründet. Darüber hinaus müsse bei der Einstellung geklärt werden, ob die Beschäftigung von Schwerbehinderten überhaupt in Frage kommen kann. Außerdem erfordere der wechselnde Einsatz bei unterschiedlichen Entleihbetrieben, Arbeitsplätzen sowie Arbeitsbedingungen die Rücksichtnahme auf evtl. Schwerbehinderungen. Weiter wurde erklärt, im Rahmen der Fürsorgepflicht müsse gefragt werden, auf welche Beeinträchtigungen und Behinderungen Rücksicht genommen werden müsse.

Es handelt sich bei diesen Daten um Gesundheitsdaten, die als besondere Arten von Daten nach § 3 Abs. 9 BDSG im Bewerbungs- bzw. Arbeitsverhältnis nur unter den Voraussetzungen des § 28 Abs. 6 bis 8 BDSG verarbeitet werden dürfen, u. a. mit Einwilligung der Bewerber bzw. Arbeitnehmer, oder wenn dies zum Zweck der Gesundheitsvorsorge oder Ähnlichem erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal erfolgt. Diese Voraussetzungen liegen hier nicht vor.

Außerdem ist die Erhebung von Daten zur Schwerbehinderung durch die Aufnahme des Diskriminierungsverbots in § 81 Abs. 2 Sozialgesetzbuch IX (Rehabilitation und Teilhabe Behinderter) seit In-Kraft-Treten dieser Regelung im Jahr 2001 nicht mehr zulässig. Die Daten dürfen im Bewerbungsverfahren nicht mehr erhoben werden. Es reicht aus und stellt keine Benachteiligung im Sinne der vorgenannten Vorschrift dar, wenn beim Bewerber Daten darüber erhoben werden, ob er körperlich und gesundheitlich in der Lage ist, die vorgesehenen Tätigkeiten zu verrichten. Im Übrigen hängt die Schwerbehindertenquote von der Gesamtzahl der Beschäftigten ab und darf frühestens ermittelt werden, wenn eine Einstellung bereits erfolgt ist und die Quote gemeldet werden muss.

Erst nach erfolgter Einstellung ist der Arbeitgeber befugt, nach einer Schwerbehinderung zu fragen, soweit sie beim Einsatz in den verschiedenen Tätigkeitsbereichen berücksichtigt und die Schwerbehindertenquote ermittelt werden muss.

Angaben über Renten: Eines der Unternehmen verlangt Angaben über evtl. Renten. Diese würden erhoben, weil der Personalfragebogen u. a. der Beratung des Bewerbers diene. Viele Bewerber, die eine Rente bezögen oder sich im Vorruhestand befänden, wüssten nicht, ob und ggf. wie viel sie hinzuverdienen dürfen. Auch gäbe es Unwissenheit über die Summen der Freigrenzen etc..

Da diese Angaben für die vorgesehenen Arbeitseinsätze nicht erforderlich sind, dürfen sie nicht bzw. erst nach einer für den Bewerber positiven Entscheidung und nur auf freiwilliger Basis erhoben werden.

Angaben über das Vorliegen einer Schwangerschaft: Zur Erforderlichkeit dieser Daten hat ein Unternehmen lapidar erklärt, die Bewerberin könne ja die Beantwortung von Fragen hierüber

ablehnen oder das Vorliegen einer Schwangerschaft verneinen. Ein anderes Unternehmen hat erklärt, Informationen über die Schwangerschaft einer Bewerberin seien bedeutsam, weil ein Auftrag verloren gehen könne, wenn eine Beschäftigte für eine bestimmte Tätigkeit überlassen werden solle und zu Beginn der Aufnahme der Tätigkeit beeinträchtigt sei.

Das Bundesarbeitsgericht hat in seiner Entscheidung vom 6. Februar 2003 (Az.: 2 AZR 621/01) entschieden, dass die Frage nach einer Schwangerschaft in jedem Fall gegen das Diskriminierungsverbot verstoße und daher unzulässig sei, weil eine Schwangerschaft kein dauerhaftes Beschäftigungshindernis darstelle. Aus diesem Grunde dürfen Daten zur Schwangerschaft und zum Termin der Niederkunft nicht erhoben werden.

Vorstrafen und Delikte: Zwei der geprüften Unternehmen fragten generell nach Vorstrafen und Delikten. Hierbei wollte ein Unternehmen seiner Sorgfaltspflicht nachkommen und ein mögliches Auswahlverschulden verhindern, z. B., wenn ein wegen Alkoholmissbrauch vorbestrafter Kraftfahrer an einen Kunden überlassen würde, dies aber aufgrund der Vorstrafe nicht erlaubt sei. Bei Vorliegen von Vorstrafen werde der Bewerber nicht abgelehnt, sondern die Einsatzmöglichkeit reduziert auf Einsätze, die in keinem inneren Zusammenhang mit der Vorstrafe des Bewerbers stehen. Zudem erwarteten die Kunden der Unternehmen, dass Fragen der Sicherheit vor der Überlassung des Arbeitnehmers geklärt seien. Beispielsweise könne ein Bankkaufmann, der vor zehn Jahren in eine Scheckbetrugsaffäre verwickelt gewesen sei, niemals einer Bank angeboten werden.

Der eingangs erwähnte Fall einer Vorstrafe wegen Alkoholmissbrauch überzeugt nicht, weil die Frage nach dem Vorhandensein eines Führerscheins bzw. dessen Vorlage zur Beurteilung der Einsatzmöglichkeiten mit einem Pkw ausreicht. Regelmäßig wird ein entzogener Führerschein erst fünf Jahre nach der Verurteilung wegen Alkohol am Steuer wieder erteilt, soweit ein Arzt die Unbedenklichkeit festgestellt hat.

Bei Fragen nach Vorstrafen ist die Wahrung der Verjährungs- bzw. Tilgungsfristen nach dem Bundeszentralregistergesetz (BZRG) zur Rehabilitation der Betroffenen zu beachten. Außerdem ist abzuwägen zwischen dem berechtigten Interesse des Unternehmens, Daten zu erheben zur Beurteilung, ob der Bewerber für die vorgesehene Arbeit verwendbar ist und dem Persönlichkeitsrecht des Bewerbers, nur die Daten preiszugeben, die sich auf die vorgesehene Arbeit beziehen.

Aus diesen Gründen dürfen regelmäßig nur Angaben über das Vorliegen von Straftaten der letzten fünf Jahre und über Delikte erhoben werden, soweit sie beachtlich sind zur Prüfung der Zuverlässigkeit für die vorgesehene Arbeit, so dass die Angaben entsprechend eingegrenzt festgelegt werden müssen. Alle Straftaten der letzten Jahre sind im polizeilichen Führungszeugnis enthalten.

Die beiden Firmen haben erklärt, den Personalfragebogen entsprechend zu ändern.

Lohn- und Gehaltspfändungen: Zur Begründung wurde vorgetragen: Die Kenntnis dieser Angaben versetzt die Firma in die Lage, einen Mehraufwand an Verwaltung zu vermeiden. Dem Bewerber entstünden durch die Bejahung dieser Frage keine Nachteile.

Da diese Frage regelmäßig nicht im Zusammenhang mit den beabsichtigten Tätigkeiten von Leiharbeitnehmern steht, darf sie erst nach der Einstellung des Bewerbers gestellt werden.

Datenschutzaufhebungserklärung: In einem Unternehmen wurde Bewerbern regelmäßig die Unterzeichnung einer sog. Datenschutzaufhebungserklärung abverlangt. Hierzu habe ich darauf verwiesen, dass niemandem abverlangt werden dürfe, auf seine unabdingbaren Rechte zu verzichten.

14.5 Prüfung von privaten Sicherheitsfirmen

Im Berichtsjahr habe ich datenschutzrechtliche Prüfungen bei privaten Sicherheitsfirmen, die auch als Detekteien Informationsbeschaffung anbieten, durchgeführt. Zunächst habe ich mir ein Bild von der Infrastruktur und den getroffenen technischen und organisatorischen Maßnahmen zur Sicherung der personenbezogenen Daten verschafft.

Ich habe den Zugangsschutz zu den vorhandenen Arbeitsplätzen, den Einsatz von mobilen Endgeräten (z. B. Notebook und PDA), die Einstellungen des WLAN, die Verschlüsselung von E-Mails, den Virenschutz, die Firewall sowie die Datensicherung und Datenvernichtung geprüft.

Lediglich Verfahrensbeschreibungen lagen zum Zeitpunkt der Prüfung nicht vor und wurden im Prüfbericht von mir angefordert. Auch die Unterrichtungspflicht über gespeicherte Daten habe ich angesprochen. Die überwachten Personen erhalten in der Regel von den Überwachungsmaßnahmen erst Kenntnis, wenn eine Schadensersatzklage, Urheberrechtsklage oder polizeiliche Maßnahmen gegen sie erfolgen. Ich habe dem Geschäftsführer einer der Sicherheitsfirmen mitgeteilt, dass die neueste Rechtsentwicklung verlangt, dass der Betroffene schon frühzeitig zu unterrichten ist, nämlich sobald der Ermittlungszweck nicht gefährdet wird.

14.6 Datenschutz im Verein - neue digitale Broschüre

Immer wieder wenden sich Vorstandsmitglieder von Vereinen wie auch Vereinsmitglieder mit Datenschutzfragen an mich. Hierzu zählen u. a. Satzungsfragen, die Bekanntgabe von Jubiläen oder die Veröffentlichung von Namen in Spielplänen bis hin zur Speicherung von Mitgliederdaten auf die privaten PCs der Vorsitzenden oder die Weitergabe von Mitgliederdaten an Versicherungsvertreter.

Um das Informationsbedürfnis auf diesem Gebiet zu befriedigen, hatte ich eine Broschüre aufgelegt, die aber mittlerweile vergriffen ist. Im Berichtsjahr wurde der Inhalt dieser Broschüre aktualisiert. Die neu gestaltete Informationseinheit kann in Kürze von meiner Homepage unter „www.datenschutz.bremen.de“ abgerufen werden. Eine gedruckte Fassung ist nicht mehr vorgesehen.

14.7 Verarbeitung von Kundendaten durch Autohandelsunternehmen

Von einer anderen Datenschutzaufsichtsbehörde wurde ich im Berichtsjahr darüber informiert, dass ein bundesweit operierendes, in Bremen ansässiges Autohandelsunternehmen seine Vertragshändler aufgefordert hatte, die von ihnen im Rahmen ihrer geschäftlichen Tätigkeit erhobenen Kundendaten zu Werbezwecken an ein großes Marketingunternehmen in Deutschland weiterzuleiten. Das Autohandelsunternehmen selbst teilte mir hierzu dann näher mit, dass es gemeinsam mit dem Marketingunternehmen ein Kunden- und Interessentenkontaktprogramm mit einem Rahmenvertrag entwickelt habe, das die Vertragshändler nutzen könnten. Eine Verpflichtung zur Teilnahme bestehe für die Händler jedoch nicht. Durch von ihnen geschlossene, separate Verträge hätten die einzelnen Autohändler dann die Möglichkeit, das Marketingunternehmen mit der Verarbeitung der Daten ihrer Kunden im Rahmen des Kunden- und Interessentenkontaktprogramms zu beauftragen. Nur wenn der Kunde bei dem jeweiligen Autohändler seine schriftliche Einwilligung zur Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten erklärt hat, gebe der Autohändler die Kundendaten an das Marketingunternehmen weiter. Da es sich um eine Auftragsdatenverarbeitung handele, bleibe der jeweilige Händler auch bei der Verarbeitung der Kundendaten durch das Marketingunternehmen die für die Datenverarbeitung verantwortliche Stelle.

Bei der Prüfung der mir von dem Autohandelsunternehmen zu seinen Erläuterungen vorgelegten Unterlagen, die an die Händler weitergegeben und dort für die Teilnahme am Kunden- und Interessentenkontaktprogramm genutzt werden, stellte ich erhebliche Mängel hinsichtlich des Inhalts der Einwilligungserklärung und der Umsetzung der Vorschriften des § 11 BDSG, die bei einem Datenverarbeitungsauftrag einzuhalten sind, fest.

So waren die für die Erteilung der Einwilligungserklärung vorgesehenen Dokumente viel zu wenig auf die vorgesehene Verarbeitung der Kundendaten zugeschnitten. Die nach § 4 a Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG) vorgeschriebene Unterrichtung der Betroffenen erfolgte nur unzureichend. Die hinsichtlich der Datenverarbeitung erforderliche Transparenz für die Betroffenen bestand nicht. Außerdem wurden die Kunden nicht darüber informiert, dass sie nach § 28 Abs. 4 BDSG jederzeit die Möglichkeit haben, der Nutzung ihrer Daten für Zwecke der Werbung zu widersprechen.

Hinsichtlich des Datenverarbeitungsauftrags der einzelnen Händler an das Marketingunternehmen war insbesondere zu beachten, dass der Auftragnehmer die ihm übergebenen personenbezogenen Daten nur im Rahmen der Weisungen des Aufraggebers verarbeiten oder nutzen darf. Auch müssen vertragliche Festlegungen hinsichtlich zu ergreifender technischer und organisatorischer Sicherungsmaßnahmen bei der Datenverarbeitung im Datenverarbeitungsauftrag getroffen werden. Soll es dem Auftragnehmer ermöglicht werden, Unteraufträge zu vergeben, so muss auch dies im Datenverarbeitungsauftrag verankert werden.

Ich habe das Autohandelsunternehmen aufgefordert, das Verfahren und die Unterlagen gemäß meiner Anforderungen zu ändern.

14.8 Auskunfteien

14.8.1 Mieterwarndateien bei Auskunfteien

Ich stehe in Kontakt mit dem Landesverband Haus & Grund und großen Vermietern über Fragen der Zulässigkeit von Auskünften verschiedener Auskunfteien über künftige Mieter sowie über Fragen des Inhalts von Mitteilungen auslaufender oder gekündigter Mietverhältnisse. Diese Auseinandersetzung wird überlagert durch Gespräche, die der Düsseldorfer Kreis in diesem Zusammenhang mit Auskunfteien und Interessenvertretungen von Mietern und Vermietern führt.

Umfang der Datenerhebung zur Bonitätsprüfung: Bei der Frage, welche personenbezogenen Mieterdaten ein Mitglied eines dem Landesverband angeschlossenen Vereins im Auftrag des Vermieters von der Auskunftei InFoScore zur Bonitätsprüfung benötigt und demzufolge erheben darf, ist gem. § 28 Abs. 1 Nr. 1 i. V. m. § 4 Abs. 2 Nr. 2 a Bundesdatenschutzgesetz (BDSG) zwischen den Rechtsgütern des Vermieters und des Mietinteressenten angemessen abzuwägen.

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

Die schutzwürdigen Interessen des Mietinteressenten basieren auf der existentiellen Bedeutung einer Wohnung als Mittelpunkt des privaten Lebensbereiches und seiner rechtlichen Schutzposition.

Nach dieser Rechtsgüterabwägung müssen sich die Bonitätsprüfung und die daraus resultierende Datenerhebung durch den Vermieter bei Auskunfteien an der spezifischen Situation des anzubahnenden Mietverhältnisses orientieren. Demzufolge ist es angemessen und zulässig, wenn ein Vermieter die bei einer branchenübergreifenden Auskunftei gespeicherten Daten erhebt, soweit sie sich auf rechtskräftige Forderungen aus Mietvertragsverhältnissen beschränken.

Diese Position wird von den anderen Aufsichtsbehörden der Länder geteilt. Die Arbeitsgruppe „Auskunfteien“ der Obersten Aufsichtsbehörden der Länder hält Angaben aus öffentlichen Registern wie Schuldnerverzeichnis und Insolvenzregister wie auch die Haftanordnung für geeignet und angemessen. Darüber hinaus sind vollstreckbare Titel aus mietrechtsrelevanten Forderungen geeignet.

Zu klären war die Frage, ob im Rahmen dieser Rechtsgüterabwägung die Übermittlung weiterer Daten über vollstreckbare Forderungen, die in keinem Zusammenhang mit einem Mietverhältnis stehen, zulässig wäre. Aus diesem Grund hat eine besondere Besprechung der Arbeitsgruppe „Auskunfteien“ mit Vertretern der Auskunfteien InFoScore, Creditreform, Bürgel und einer speziellen Mieterauskunftei aus Nordrhein-Westfalen stattgefunden. Die Schufa war verhindert. Darüber hinaus nahmen an dem Gespräch Vertreter des Bundesverbandes Haus & Grund sowie des Landesverbandes der Wohnungsunternehmen Berlin/Brandenburg teil.

Die vertretenen Auskunfteien haben erklärt, sie würden an Vermieter ggf. den komplett vorhandenen Datenkatalog übermitteln. Eine Differenzierung nach Auskunftsempfängern finde nicht statt. Lediglich

die spezielle Mieterauskunftei aus Nordrhein-Westfalen übermittle nur Daten über rechtskräftige Entscheidungen aus vertragsbrüchigen Mietverhältnissen an Vermieter.

Die Vertreter der Vermieterorganisationen erklärten, sie seien an jeglicher Information in Bezug auf das Zahlungsverhalten und Informationen über nicht vertragsmäßiges Verhalten interessiert; ggf. wolle man auch beim Vorvermieter nachfragen, ob es Probleme im Mietverhältnis gegeben habe.

Nach Abschluss dieser Beratung ist beabsichtigt, demnächst mit Vertretern der seinerzeit verhinderten Schufa und dem Deutschen Mieterbund zusammenzutreffen.

Einwilligung oder Unterrichtung vor Einholung einer Auskunft: Anlässlich der vorgenannten Besprechung erklärten die Vermieterorganisationen, sie bevorzugten die Einwilligung als gesetzliche Befugnis zur Einholung einer Auskunft, um so an alle bei Auskunfteien gespeicherten Negativmerkmale zu gelangen.

Die Auskunfteien erklärten in diesem Zusammenhang, sie ließen sich bei Vermieteranfragen keine Einwilligungserklärungen vorlegen. Sie gingen davon aus, dass die Vermieter berechtigte Interessen an den Auskünften hätten.

Die Arbeitsgruppe „Auskunfteien“ der Datenschutzaufsichtsbehörden vertritt die Auffassung, dass die Einholung einer Einwilligung mit rechtlichen Risiken behaftet ist. Es könne nicht ausgeschlossen werden, dass diese aufgrund der eingangs erwähnten existentiellen Bedeutung einer Wohnung als Mittelpunkt des privaten Lebensbereiches regelmäßig nicht freiwillig sei, insbesondere, wenn sie formularmäßig eingeholt würde und damit nicht die Besonderheiten des Einzelfalles berücksichtige. Die Einholung bei einer Auskunftei sollte daher grundsätzlich auf Grundlage der §§ 28, 29 BDSG erfolgen und die Mietinteressenten darüber vorher unterrichtet werden. Diese könnten dann entscheiden, ob sie an einer weiteren Anbahnung eines Mietvertragsverhältnisses interessiert seien.

Verzicht auf Solvenzprüfung bei Mietübernahmegarantie: In Bremen holten Wohnungsunternehmen Auskünfte über Mietinteressenten, die gleichzeitig Sozialhilfeempfänger sind, bei der Schufa und anderen Auskunfteien hinsichtlich dort vorhandener Negativmerkmale ein, auch wenn eine Mietübernahmebescheinigung des Sozialamtes vorlag. Aufgrund der Vielzahl und der unterschiedlichen Praxis der Wohnungsunternehmen in Bremen habe ich dem Landesverband der Wohnungswirtschaft in Bremen/Niedersachsen meine Rechtsauffassung hierzu dargelegt.

Da es sich hierbei um eine Erhebung personenbezogener Daten bei anderen Stellen als den Betroffenen handelt, ist eine Anfrage des Vermieters bei einer Auskunftei nach § 28 Abs. 1 Satz 1 Nr. 1 i. V. m. § 4 Abs. 2 Nr. 2 a BDSG nur zulässig, wenn die Anfrage für die Prüfung der Solvenz des Mietinteressenten erforderlich ist und dessen schutzwürdige Interessen nicht überwiegen.

Zulässig wäre eine solche Auskunftseinholung nur dann, wenn keine Garantien oder sonstigen Sicherheiten vorliegen, die das wirtschaftliche Risiko des Wohnungsunternehmens bei fehlender Solvenz des Mietinteressenten auf ein vertretbares Maß reduzieren würden. Hierbei ist abzuwägen zwischen der Wahrung des vertretbaren Risikos des Vermieters und den schutzwürdigen Interessen des Mietinteressenten aufgrund seiner grundrechtlichen Schutzposition aus Art. 2, 13 und 14 Grundgesetz (GG) und den Vorschriften des einfachen Mietrechts.

Da allerdings in den hier zugrunde liegenden Fällen Garantien bzw. Sicherheiten in Form von Mietübernahmebescheinigungen der Sozialhilfeträger vorliegen, sind Anfragen bei Auskunfteien nicht erforderlich; es überwiegen insoweit regelmäßig schutzwürdige Interessen der betroffenen Mietinteressenten. Demzufolge ist diese Datenerhebung nicht zulässig.

Der Verband hat daraufhin erklärt, aufgrund der unterschiedlichen Verfahrensweisen seiner Mitgliedsunternehmen sei eine einheitliche Stellungnahme schwierig. Außerdem sei eine rechtliche Beurteilung derzeit nicht abschließend möglich, weil die zugrunde liegenden Rechtsvorschriften zum 1. Januar 2005 komplett umgestellt würden (Hartz IV).

Anlässlich der vorgenannten Besprechung der Aufsichtsbehörden erklärten die Vertreter der Wohnungswirtschaft, bei Vorliegen einer Mietgarantie eines Dritten sei eine Prüfung der Solvenz, namentlich eine Anfrage bei einer Auskunftei, nicht erforderlich.

14.8.2 Creditreform Bremen

Im vergangenen Jahr erhielt ich wieder mehrere Eingaben, die die Verarbeitung personenbezogener Daten durch die Auskunftei Creditreform Bremen betrafen. Von der Datenverarbeitung der Auskunftei betroffene Bürger und Bürgerinnen beklagten sich u. a. darüber, dass sie ihre Betroffenenrechte nicht hinreichend wahrnehmen können, ihre Daten unzulässigerweise gespeichert würden oder ohne erkennbaren Grund an einen Dritten übermittelt worden seien. Erst durch meine aufsichtsbehördliche Tätigkeit konnte vielfach erreicht werden, dass die Betroffenen die von ihnen erbetene Auskunft erhielten oder aber die Zulässigkeit der Datenverarbeitung geklärt wurde.

Beklagt hatte sich eine Petentin bei mir u. a. auch darüber, dass zu ihrer Person sog. Schätzdaten gespeichert würden. Schätzdaten sind Daten, die branchenübliche Durchschnittswerte darstellen, und soweit keine konkreten Angaben im Einzelfall vorhanden sind, den Angaben zur Person des Betroffenen hinzugefügt und auch an Dritte übermittelt werden. Im Fall meiner Petentin waren u. a. Durchschnittswerte zur Geschäftsentwicklung, zu den Umsätzen des Unternehmens und zur Betriebs- und Geschäftsausstattung gespeichert.

Die Zulässigkeit der Verarbeitung von Schätzdaten ist umstritten. Problematisch ist insbesondere, dass durch die Speicherung von Schätzdaten möglicherweise ein unrichtiges Bild über den Betroffenen geschaffen wird. Nach kontroverser Diskussion, insbesondere mit Vertretern des Verbandes der Handelsauskunfteien, hat man sich in der AG Auskunfteien des Düsseldorfer Kreises schließlich auf eine besondere Kennzeichnung der Daten durch einen speziellen Hinweis, dass es sich um branchenübliche Durchschnittswerte handele, geeinigt. Eine solche besondere Kennzeichnung enthielten auch die zur Petentin gespeicherten Schätzdaten, so dass ich die Speicherung der Daten in diesem Fall nicht beanstanden konnte.

In den Fällen, in denen sich Petenten bei mir darüber beklagten, dass ihnen die Wahrnehmung ihrer Betroffenenrechte verwehrt werde, konnte ich ihnen zur Durchsetzung der ihnen nach § 34 Bundesdatenschutzgesetz (BDSG) zustehenden Rechte verhelfen. In einem Fall, in dem ohne erkennbaren Grund personenbezogene Daten des Betroffenen an ein Kreditversicherungsunternehmen übermittelt wurden, konnte ich dies zwar nicht rückgängig machen, ich habe aber den Datenübermittlungsvorgang für den Betroffenen transparent gemacht und für Löschung der Daten gesorgt.

14.8.3 Datenübermittlung durch die Schufa an Versandhandelsunternehmen

Seit dem 1. Januar 2002 hat die Schufa eine neue Unternehmensstruktur (vgl. 25. JB, Ziff. 14.13.2). Die bis dahin rechtlich selbständigen Regionalgesellschaften, davon eine mit Sitz in Bremen, wurden zur Schufa Holding AG verschmolzen. Diese hat ihren Sitz in Wiesbaden. Das hat zur Folge, dass für die Datenschutzaufsicht über die Schufa allein das Regierungspräsidium Darmstadt zuständig ist. Eine Kontroll- und Beratungskompetenz meiner Dienststelle besteht nicht mehr.

Das bedeutet freilich nicht, dass mich die Schufa nicht mehr beschäftigt. Im Rahmen des Düsseldorfer Kreises, des ständigen Koordinationsgremiums der obersten Aufsichtsbehörden der Länder für den Datenschutz, werden nach wie vor wichtige datenschutzrechtliche Fragen erörtert, die den Umgang mit personenbezogenen Daten in Auskunfteien und besonders bei der Schufa betreffen.

Im Berichtsjahr ist u. a. Folgendes in der Arbeitsgruppe „Auskunfteien“ des Düsseldorfer Kreises diskutiert worden: Die Aufsichtsbehörden haben festgestellt, dass Versandhändler, die in einer Geschäftsbeziehung mit der Schufa stehen, von dort Auskünfte über Betroffene einholen, die einen Bestellwunsch an sie richten. Dabei melden sie der Schufa das Merkmal „VK“. Damit erklären sie, dass ein Kunde bei ihnen ein Versandhauskonto führt, obwohl der Betroffene u. U. nur eine einzige Bestellung vorgenommen hat und auch keine weiteren Bestellungen beabsichtigt. Dennoch übermittelt die Schufa, solange das Merkmal „VK“ dort für den Betroffenen gespeichert ist (in der Regel 12 Monate), im Rahmen von so genannten Nachmeldungen personenbezogene Daten, die Aufschluss über die Kreditwürdigkeit geben, an die Versandhändler. Bei den Nachmeldungen handelt es sich um Informationen, die nachträglich bekannt werden und die ursprüngliche Auskunft ergänzen. Auf diese Weise erhalten Versandhandelsunternehmer z. T. sensible Daten über Kunden im Nachhinein, obwohl diese vielleicht nur ein einziges Mal mit dem Händler in Kontakt getreten sind.

Der Düsseldorfer Kreis hält diese Verfahrensweise für nicht mit den Vorschriften des Bundesdatenschutzgesetzes (BDSG) vereinbar, weil der Versandhändler kein berechtigtes Interesse hat, Nachmeldungen über den Betroffenen zu erhalten. Ich unterstütze diese Position. Die Argumentation der Schufa, nach den Erfahrungen des Versandhandels handele es sich bei der großen Mehrheit der Kunden um Mehrfach-Besteller, lehne ich ab. Die Schufa muss das Merkmal „VK“ und die entsprechenden Voraussetzungen über die Meldung des Merkmals so klar definieren, dass die Auslegung und Handhabung der Meldung nicht im Belieben der Versandhändler steht. Denn sie trägt die Verantwortung für die ordnungsgemäße Datenübermittlung und muss das „berechtigte Interesse“ ihrer Vertragspartner stichprobenartig überprüfen. Auf Druck der Aufsichtsbehörden hat die Schufa diesen gegenüber erklärt, sie werde sich um eine exaktere Definition des Merkmals „VK“ bemühen.

14.9 Verarbeitung von Lkw-Mautdaten

Seit dem 1. Januar 2005 wird die Lkw-Maut erhoben. Bis zur Einführung war ein langer Weg mit häufig ungewissem Ausgang zurückzulegen. Grundlage dieser Mauterhebung ist das Gesetz zur Einführung von streckenbezogenen Gebühren für die Benutzung von Bundesautobahnen mit schweren Nutzfahrzeugen (Autobahnmautgesetz für schwere Nutzfahrzeuge – ABMG) vom 5. April 2002 (BGBl. I S. 1234). Eine Neufassung des ABMG erfolgte am 2. Dezember 2004 (BGBl. I S. 3122 ff.).

Zuständigkeit auch der Aufsichtsbehörden für den Datenschutz: Das ABMG verpflichtet alle Mautschuldner, die erforderlichen Daten über Fahrzeiten und -routen auf Autobahnen anzugeben. Durch daraufhin erfolgende Abrechnungen nehmen die Speditionsfirmen Kenntnis von personenbezogenen Daten über ihre Beschäftigten, soweit diese als Fahrer auf den jeweiligen Lkws des Unternehmens eingesetzt werden.

Nicht auszuschließen ist, dass die Mautschuldner in ihrer Funktion als Arbeitgeber die Daten für Leistungs- und Verhaltenskontrollen verwenden, obwohl dies nach den Regelungen im ABMG über die Zweckbindung der Mautdaten unzulässig wäre (siehe nachstehende Ausführungen). Gleichwohl wären insoweit die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) zumindest zu prüfen, so dass nicht ausgeschlossen ist, dass sich neben dem Bundesbeauftragten für den Datenschutz (BfD), als Kontrollstelle für die im ABMG genannten Bundesbehörden und dem Betreiber, auch die Aufsichtsbehörden für den Datenschutz, als Kontrollstelle für die Arbeitgeber, mit dieser Problematik befassen werden.

Dabei wird und soll auch nicht originär die Zuständigkeit des BfD berührt werden. Mit Fragen der Verwendung von Mautdaten durch Mautschuldner als Arbeitgeber für Leistungs- und Verhaltenskontrollen hat sich bereits der Workshop der Aufsichtsbehörden für den Datenschutz im letzten Jahr in Bremen befasst.

Gesetzliche Regelungen zur Datenverarbeitung: Nach § 4 Abs. 2 ABMG kann das Bundesamt für Güterverkehr die Errichtung und den Betrieb eines Systems zur Erhebung der Maut einem Privaten anordnen, was durch die Übertragung an die Firma Toll Collect als Betreiber geschehen ist. Im ABMG wird normenklar und abschließend geregelt, welche personenbezogenen Daten über die Lkw-Unternehmen (Mautschuldner) der Betreiber zum Betrieb des Mauterhebungssystems erheben, verarbeiten und nutzen darf. Ausdrücklich ist gesetzlich festgelegt worden, dass die Mautdaten nur

- für den Betrieb des Mauterhebungssystems und die Erhebung der Maut durch den Betreiber,
- zum Nachweis der Mautentrichtung durch den Mautschuldner und
- zur Überwachung der Einhaltung des ABMG durch das Bundesamt für den Güterverkehr und die Zollbehörden

verarbeitet werden dürfen.

Mit einer Entschließung der Konferenz der Datenschutzbeauftragten vom Oktober 2001 zur Lkw-Maut ist die Bundesregierung aufgefordert worden, bei der technischen Realisierung datenschutzrechtliche Anforderungen durchzusetzen (vgl. 24. JB, Ziff. 15.12).

Technische Umsetzung des Mauterhebungssystems: Nach Auswertung verschiedener Publikationen ergibt sich folgendes Bild. Vorgesehen ist zum einen, dass in jedem in Deutschland verkehrenden Lkw eine sog. On-Board Unit (OBU) eingebaut wird. Dieses Gerät entspricht der Größe eines Autoradios. Es wird an die Bordelektronik angeschlossen und mit einem Tachosensor, einem GPS-Empfänger, einer GSM-Antenne und einem Infrarotsender ausgestattet. Die OBU vergleicht ständig die aktuellen GPS-Koordinaten mit einer im Gerät gespeicherten Straßenkarte von Deutschland. Sobald erkannt wird, dass der Lkw auf eine mautpflichtige Autobahn gefahren ist, beginnt der Gebührenzähler zu laufen. Anhand der GPS-Daten und dem Tachosignal wird die Plausibilität der gemessenen Werte überprüft. Zudem ist in jede OBU ein GSM-Telefon (Handy) integriert, welches sich wie ein herkömmliches Mobilfunkgerät im Mobilfunknetz von T-Mobile einbucht. Verlässt der Lkw die mautpflichtige Strecke, wird per GSM eine Mitteilung mit der errechneten Maut an das Toll Collect-Rechenzentrum geschickt, die diese Daten sammelt und dem Mautschuldner (Transportunternehmen) in Rechnung stellt.

Der Betreiber Toll Collect hat insgesamt ca. 300 sog. Maut-Brücken an allen Autobahnen in Deutschland aufgestellt. Damit soll kontrolliert werden, ob im Lkw tatsächlich eine OBU mit laufendem Gebührenzähler eingebaut ist. Dazu sollen zunächst die Frontbilder und Kennzeichen sämtlicher Kfz - also auch aller Pkw - per Videokamera erfasst und automatisch ausgewertet werden, wobei die Kfz-Kennzeichen auf den Frontbildern erkannt und separiert bzw. zwischengelagert werden sollen. Sobald ein Lkw mit OBU auf die Kontrollbrücke zufährt, wird die OBU per Infrarot-Signal aufgefordert, sich zu identifizieren. Ergibt diese Kommunikation, dass die OBU eingeschaltet ist und Gebühren berechnet werden, sollen die Videobilddaten sofort wieder gelöscht werden. Beim Durchfahren der Kontrollbrücke sollen die Fahrzeuge mittels Laser vermessen werden, um festzustellen, ob das Fahrzeug mautpflichtig ist. Dabei soll der Umriss des Kfz ausschlaggebend sein. Wird dabei keine Mautpflicht festgestellt, sollen die Videobilddaten auch dieser Kfz wieder gelöscht werden.

Zum anderen ist geplant, dass insbesondere ausländische Transportunternehmen über Internet oder an ca. 3.500 Mautstellen-Terminals an Tankstellen, vorwiegend an Autobahnen, vorab ihre Maut entrichten können. Dazu muss die Fahrtroute vorher gebucht werden. Wenn ein derartiges Fahrzeug eine Kontrollbrücke passiert und als solches erkannt wird, soll das automatisch ausgelesene Kfz-Kennzeichen mit der Datenbank der manuell eingebuchten Fahrtrouten verglichen werden. Wenn es dabei nicht zu einem „Treffer“ kommt, soll das aufgenommene Foto des Fahrzeugs als Beweismittel für einen Bußgeldbescheid verwendet werden.

Außerdem soll das Bundesamt für den Güterverkehr (BAG) über eine Kontrollschnittstelle „Auftraggeber“ einen elektronischen Zugriff auf sämtliche Fahrtrouten der letzten Jahre erhalten.

Ferner soll die zentrale Datenbank von Toll Collect Einzelüberwachungsmaßnahmen durch das BAG ermöglichen. Dabei werden in der Datenbank sog. Trigger gesetzt, die Alarm schlagen, wenn ein bestimmtes Kfz-Kennzeichen durch die Meldung der OBU oder durch Video-Identifikation erscheint.

Besondere Risiken für die Rechte und Freiheiten der Betroffenen durch die Mautdatenverarbeitung

Die vorgenannte technische Umsetzung zeigt, dass die Anforderungen der Datenschutzbeauftragen nur unzureichend beachtet worden sind. Insbesondere widerspricht es dem Grundsatz der Datenvermeidung, wenn nicht nur mautpflichtige Lkw, sondern sämtliche Kfz per Video aufgenommen werden, auch wenn beabsichtigt ist, die von vornherein nicht erforderlichen Daten sofort wieder zu löschen, wenn sie nicht mehr benötigt werden. Technisch möglich bleibt, die Löschung durch eine Änderung des Programms zu unterbinden. Damit ist es technisch nicht ausgeschlossen, einen Datenbestand über alle die Autobahnen nutzenden Lkw und Pkw zu erstellen und für vielfältige Zwecke zu nutzen.

Zwar ist der Grundsatz der Zweckbindung mehrfach ausdrücklich im Gesetz aufgeführt. Gleichwohl hat das Amtsgericht Gummersbach mit Beschluss vom 31. August 2003 – 10 a Gs 2399/03 – entschieden, die Firma Toll Collect und das Bundesamt für Güterverkehr seien als Mitwirkende an der geschäftsmäßigen Erbringung von Telekommunikationsdienstleistungen verpflichtet, auf richterliche Anordnung unter den Voraussetzungen der §§ 100 g, 100 h Strafprozessordnung (StPO) die Standortdaten der in einem Mauterfassungsgerät eines Fahrzeugs installierten GIS-SIM-Karte herauszugeben.

Das Amtsgericht hatte ausgeführt, das im AMBG verankerte Datenverarbeitungs- und Verwertungsverbot sei im Lichte der vorgenannten Vorschriften der StPO auszulegen; ein allgemeines Verwertungsverbot könne dem Gesetz nicht entnommen werden.

Im Gegensatz zum Bundesministerium des Innern haben dieser Auffassung u. a. der Datenschutzbeauftragte der Betreiberin, der Bundesbeauftragte für den Datenschutz sowie die Bundesministerien für Justiz und für Verkehr, Bau- und Wohnungswesen widersprochen.

Der Bundesbeauftragte für den Datenschutz hat gegenüber dem Ausschuss für Verkehr, Bau und Wohnungswesen geäußert, in §§ 4 Abs. 2 Satz 5 und 7, Abs. 2 Satz 3 ABMG vom 2. Dezember 2004 (BGBl. I S. 3122 ff.) sei ergänzend und präzise geregelt worden, dass „eine Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften unzulässig ist“ (BT-Drs. 15/3819 vom 29. September 2004 S. 6).

Trotz dieser materiell-rechtlichen Klarstellung vor der geplanten Einführung der Lkw-Maut bleibt abzuwarten, ob der Damm einer rechtlichen Nutzungsbeschränkung der Daten hält.

14.10 Workshop der Datenschutz-Aufsichtsbehörden

Im September des Berichtsjahres war ich Gastgeber des Workshops der Datenschutz-Aufsichtsbehörden für den nicht öffentlichen Bereich, an dem Vertreter von Aufsichtsbehörden aus fast allen Bundesländern teilnahmen. Der Workshop, der jährlich und abwechselnd in den verschiedenen Ländern veranstaltet wird, befasste sich auch diesmal mit einer Vielzahl aktueller den Datenschutz betreffender Themen, die einer gemeinsamen Diskussion dringend bedurften.

Diskutiert wurden u. a. die Überwachung der Internet- und der E-Mail-Nutzung des Arbeitnehmers durch den Arbeitgeber, die nicht selten mit einem erheblichen Eingriff in die Arbeitnehmerrechte verbunden ist, Fragen der Veröffentlichung personenbezogener Daten im Internet, die Nutzung biometrischer Verfahren zur Zugangskontrolle sowie die bei der Bestellung von betrieblichen Datenschutzbeauftragten bei Kleinunternehmen und Freiberuflern (z. B. Arztpraxen, Apotheken, Steuerberater- und Rechtsanwaltskanzleien) zu beachtenden datenschutzrechtlichen Anforderungen.

Näher erörtert wurde von den Workshop-Teilnehmern darüber hinaus u. a. die oftmalige Weigerung der Auskunfteien, dem Betroffenen Auskunft auch über den Empfänger seiner Daten zu erteilen mit dem Hinweis, das Geschäftsgeheimnis überwiege den Auskunftsanspruch des Betroffenen. Die Teilnehmer des Workshops gelangten hierbei zu der Auffassung, dass grundsätzlich in jedem Einzelfall zu prüfen sei, ob das Interesse an der Wahrung des Geschäftsgeheimnisses das Auskunftsinteresse des Betroffenen überwiegt. Eine generelle Auskunftsverweigerung sei jedenfalls nicht zulässig.

Im Hinblick auf die Durchführung von Video-Überwachungsmaßnahmen kamen die Vertreter der Aufsichtsbehörden u. a. überein, dass der Einsatz von Webcams in gastronomischen Einrichtungen grundsätzlich nur dann unbedenklich ist, wenn Personen nicht mehr identifizierbar sind, z. B. durch Übersichtsaufnahmen, Unschärfe etc..

Besondere Aufmerksamkeit fanden bei den Workshop-Teilnehmern schließlich Vorträge im Rahmen der Veranstaltung, die ein betrieblicher Datenschutzbeauftragter über die Praxis seiner Amtswahrnehmung sowie technische Mitarbeiter des Hamburgischen Datenschutzbeauftragten und des Technologie-Zentrums Informatik der Universität Bremen zur Sicherheit im WLAN hielten.

14.11 Verfahrensregister

Mit der Novelle des Bundesdatenschutzgesetzes (BDSG) verbunden ist eine grundlegende Veränderung der Regelungen zur Registerführung durch die Datenschutzaufsichtsbehörden. Ich habe daher alle bisher im Register verzeichneten nicht öffentlichen Stellen auf deren Meldepflicht überprüft.

Derzeit werden im Verfahrensregister sechs Stellen geführt, wobei es sich um drei Auskunfteien, zwei Markt- und Meinungsforschungsinstitute und ein Adresshandelsunternehmen handelt. Das Register kann von jedermann bei mir eingesehen werden.

14.12 Ordnungswidrigkeitenverfahren

Trotz wiederholter Aufforderung habe ich von zwei EDV-Unternehmen und einem Markt- und Meinungsforschungsinstitut keine Antworten auf meine Schreiben erhalten, obwohl sie nach § 38 Abs. 3 Satz 1 Bundesdatenschutzgesetz (BDSG) verpflichtet sind, mir unverzüglich die erforderlichen Auskünfte zu erteilen. Gegen diese Firmen habe ich Bußgeldverfahren eingeleitet. Diese führten immerhin dazu, dass ich von den betreffenden Stellen die angeforderten Auskünfte schließlich erhielt. Die Bußgelder wurden zum überwiegenden Teil bereits gezahlt.

15. Die Entschließungen der Datenschutzkonferenzen im Jahr 2004

15.1 Personennummern

(Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004)

Das Bundesverfassungsgericht hat schon in seinem „Volkszählungsurteil“ aus dem Jahre 1983 besonders betont, dass ein Personenkennzeichen nicht verfassungsgemäß ist. Deshalb gibt die Einführung von einheitlichen Personennummern z. B. im Steuerbereich oder auch im Arbeits-, Gesundheits- und Sozialbereich Anlass zu grundsätzlicher Kritik. Der Staat darf seine Bürgerinnen und Bürger nicht zur Nummer abstempeln. Durch die technische Entwicklung sind vorhandene Dateien leicht miteinander zu verknüpfen und könnten zu einer vom Bundesverfassungsgericht strikt abgelehnten allgemeinen Personennummer führen.

Die Konferenz appelliert an die Gesetzgeber, solche Personennummern zu vermeiden. Soweit jedoch im Einzelfall derartige Nummern unerlässlich sind, muss der Gesetzgeber strenge Zweckbindungen und Verwendungsverbote vorsehen.

15.2 Übermittlung von Flugpassagierdaten an die US-Behörden

(Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004)

Die Datenschutzbeauftragten des Bundes und der Länder bestärken die Bundesregierung darin, sich für Verbesserungen des Datenschutzes bei der Übermittlung von Flugpassagierdaten an die Zoll- und Sicherheitsbehörden der USA einzusetzen.

Durch einseitigen Rechtsakt haben die USA die Fluggesellschaften, die ihr Land anfliegen, unter Androhung teilweise empfindlicher Strafen verpflichtet, den US-Zoll- und Sicherheitsbehörden den Zugang zu ihren Reservierungsdatenbanken zu eröffnen, um anhand der darin enthaltenen Informationen über die Fluggäste mögliche terroristische oder kriminelle Aktivitäten frühzeitig zu erkennen. In den Reservierungsdatenbanken halten die an der Reisedurchführung beteiligten Stellen alle Informationen fest, die sie benötigen, um die Flugreise abzuwickeln. Es werden z. B. Name, Reiseverlauf, Buchungsstelle, Art der Bezahlung, bei Zahlung mit Kreditkarte deren Nummer, Sitzplatz, Essenswünsche, notwendige Reisevorkehrungen wegen einer Erkrankung eines Fluggastes, Hotel- und Mietwagenreservierungen im Buchungssystem gespeichert. Teilweise sind die gespeicherten Daten sensitiv, weil sie Rückschlüsse auf die Gesundheit einzelner Fluggäste oder religiöse oder politische Anschauungen ermöglichen.

Die US-Zollbehörden wollen alle Reservierungsdaten mindestens dreieinhalb Jahre speichern ungeachtet der Tatsache, ob gegen eine Person ein Verdachtsmoment vorlag oder nicht. Passagierdaten, die im Einzelfall überprüft wurden, sollen zudem weitere acht Jahre gespeichert werden.

Die Datenschutzbeauftragten verkennen nicht, dass nach den Ereignissen des 11. September 2001 ein erhöhtes Bedürfnis nach Sicherheit im Flugverkehr offensichtlich ist. Sie verschließen sich deshalb keineswegs Forderungen, die auf eine sichere Identifikation der Fluggäste zielen. Dennoch muss festgestellt werden, dass die Forderungen der USA weit über das hinausgehen, was erforderlich ist. Da die Reservierungsdatenbanken nicht für Sicherheitszwecke, sondern zur Durchführung der Flugreisen angelegt werden, enthalten sie auch eine Vielzahl von Daten der Reisenden, die für eine Sicherheitsüberprüfung der Passagiere irrelevant sind.

Mit dem Zugriff ist wegen der teilweise hohen Sensibilität der Daten ein tiefer Eingriff in die Persönlichkeitsrechte der Betroffenen verbunden. Besonders hervorzuheben ist in diesem Zusammenhang, dass die US-Behörden hier aufgrund US-amerikanischen Rechts auf Datenbanken außerhalb ihres Hoheitsbereichs zugreifen. Die betroffenen Personen werden gegenüber dem Zugriff auf ihre Daten durch eine ausländische Stelle in ihren Datenschutzrechten weitgehend schutzlos gelassen. Ein vergleichbares Ansinnen deutscher Sicherheitsbehörden wäre schwerlich mit unserer Verfassung vereinbar.

Die Problematik kann sich weiter verschärfen, wenn die USA die Passagierdaten zukünftig auch im sog. CAPPS II – System einsetzen wollen. Dieses System ermöglicht sowohl einen automatisierten

Abgleich mit Fahndungslisten als auch mit Informationen aus dem privaten Sektor. Insbesondere sollen Kreditkarten- und Adressdaten mit Informationen aus der Kreditwirtschaft abgeglichen werden.

Die Europäische Kommission bemüht sich seit über einem Jahr in Verhandlungen darum, den Datenzugang der US-Behörden auf ein angemessenes Maß zu beschränken. Leider führten die Verhandlungen nur in Teilbereichen zum Erfolg. Die erzielten Ergebnisse in ihrer Gesamtheit gewähren den Reisenden keinen angemessenen Schutz ihrer Persönlichkeitsrechte. Dies hat die Gruppe nach Art. 29 der europäischen Datenschutzrichtlinie (EG-DSRL) in ihrer Stellungnahme vom 29. Januar 2004 deutlich herausgearbeitet:

(http://www.europa.eu.int/comm/internal_market/privacy/workingroup/wp2004/wpdocs04_de.htm)

Die darin vertretenen Positionen werden von den Datenschutzbeauftragten ausdrücklich unterstützt. Dennoch beabsichtigt die Europäische Kommission das Ergebnis ihrer Verhandlungen als einen angemessenen Datenschutzstandard förmlich anzuerkennen. Die Datenschutzbeauftragten appellieren an die Bundesregierung, sich gegen diese Entscheidung der Kommission zu wenden. Wenn die Kommission diesen unbefriedigenden Verhandlungsergebnissen ein angemessenes Datenschutzniveau attestiert, setzt sie damit Maßstäbe sowohl für die Auslegung der EU-Datenschutzrichtlinie als auch für Verhandlungen mit anderen Staaten über die Anerkennung des dortigen Datenschutzniveaus. Die Bundesregierung sollte sich demgegenüber für eine Lösung einsetzen, die Sicherheitsaspekte und den Schutz der Persönlichkeitsrechte in ein angemessenes Verhältnis setzt. Insbesondere sind die Informationen ausdrücklich zu benennen, die für die Passagieridentifikation benötigt werden. Diese Daten können zu einem angemessenen Zeitpunkt vor dem Abflug bereitgestellt werden. Ein unmittelbarer pauschaler Zugriff auf europäische Datenbanken, wie er zurzeit praktiziert wird, muss ausgeschlossen werden.

15.3 Radio-Frequency Identification

(Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder schließt sich voll inhaltlich der folgenden Entschließung an:

Entschließung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre - Entschließung zu Radio-Frequency Identification vom 20. November 2003

(Übersetzung)

Radio-Frequency Identification (RFID) Technologie wird zunehmend für eine Reihe unterschiedlicher Zwecke eingesetzt. Während es Situationen gibt, in denen diese Technologie positive und günstige Auswirkungen hat, sind auch negative Folgen für Privatsphäre möglich. RFID-Etiketten werden bisher vorwiegend zur Identifikation und Organisation von Gegenständen (Produkten), zur Kontrolle der Logistik oder zum Schutz der Authentizität einer Produktmarke (Warenzeichen) verwendet; sie können aber auch mit personenbezogenen Informationen wie Kreditkarten-Daten verknüpft werden und auch zur Erhebung solcher Informationen oder zur Lokalisierung oder Profilbildung über Personen benutzt werden, die Gegenstände mit RFID-Etiketten besitzen. Diese Technologie würde die unbemerkte Verfolgung und das Aufspüren von Individuen ebenso wie die Verknüpfung erhobener Daten mit bestehenden Datenbanken ermöglichen.

Die Konferenz hebt die Notwendigkeit hervor, Datenschutzprinzipien zu berücksichtigen, wenn RFID-Etiketten verknüpft mit personenbezogenen Daten eingeführt werden sollen. Alle Grundsätze des Datenschutzrechts müssen beim Design, der Einführung und der Verwendung von RFID-Technologie berücksichtigt werden. Insbesondere

- sollte jeder Datenverarbeiter vor der Einführung von RFID-Etiketten, die mit personenbezogenen Daten verknüpfbar sind oder die zur Bildung von Konsumprofilen führen, zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen;
- wenn der Datenverarbeiter darlegen kann, dass personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden;
- dürfen personenbezogene Daten nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und sie dürfen nur solange aufbewahrt werden, wie es zur Erreichung dieses Zwecks erforderlich ist und
- soweit RFID-Etiketten im Besitz von Personen sind, sollten diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten haben.

Diese Grundsätze sollten bei der Gestaltung und bei der Verwendung von Produkten mit RFID berücksichtigt werden.

Das Auslesen und die Aktivierung von RFID-Etiketten aus der Ferne ohne vernünftige Gelegenheit für den Besitzer des etikettierten Gegenstandes, diesen Vorgang zu beeinflussen, würde zusätzliche Datenschutzrisiken auslösen.

Die Konferenz und die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die technischen Entwicklungen in diesem Bereich genau und detaillierter verfolgen, um die Achtung des Datenschutzes und der Privatsphäre in einer Umgebung allgegenwärtiger Datenverarbeitung sicherzustellen.

15.4 Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff und zur präventiven Telekommunikationsüberwachung

(Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004)

Das Urteil des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff ist ein wichtiger Orientierungspunkt in der rechts- und sicherheitspolitischen Diskussion um den sachgerechten Ausgleich zwischen dem staatlichen Auftrag zur Verfolgung und Verhütung von Straftaten einerseits und dem Schutz der grundgesetzlich garantierten Bürgerrechte andererseits. Das Urteil bekräftigt den hohen Rang des Grundrechts auf Unverletzlichkeit der Wohnung und des Rechts auf informationelle Selbstbestimmung. Das Gericht betont, dass der absolut geschützte Kernbereich privater Lebensgestaltung nicht zugunsten der Strafverfolgung eingeschränkt werden darf. Damit darf es keine Strafverfolgung um jeden grundrechtlichen Preis geben.

Die Ausführungen des Bundesverfassungsgerichts sind nicht nur für die Vorschriften über die akustische Wohnraumüberwachung in der Strafprozessordnung von Bedeutung. Auf den Prüfstand müssen jetzt auch andere Eingriffsbefugnisse, wie etwa die Telekommunikationsüberwachung und andere Formen der verdeckten Datenerhebung mit zwangsläufigen Berührungen zum Bereich privater Lebensgestaltung gestellt werden, wie etwa die längerfristige Observation, der verdeckte Einsatz technischer Mittel, der Einsatz von Vertrauenspersonen oder von verdeckten Ermittlern. Hiervon betroffen sind nicht nur Bundesgesetze, sondern beispielsweise auch die Polizei- und Verfassungsschutzgesetze der Länder.

Insbesondere angesichts zunehmender Bestrebungen, auch die Telefonüberwachung für präventive Zwecke in Polizeigesetzen zuzulassen, ist darauf hinzuweisen, dass das Bundesverfassungsgericht in einem Beschluss zum Außenwirtschaftsgesetz ebenfalls am 3. März 2004 der präventiven Überwachung des Postverkehrs und der Telekommunikation klare Grenzen gesetzt hat.

Die Datenschutzbeauftragten fordern die Gesetzgeber des Bundes und der Länder deshalb auf, zügig die einschlägigen Vorschriften nach den Maßstäben der verfassungsgerichtlichen Entscheidungen vom 3. März 2004 zu korrigieren. Die mit der praktischen Durchführung der gesetzlichen Eingriffsbefugnisse befassten Gerichte, Staatsanwaltschaften und Polizeien sind aufgerufen, die Vorgaben des Bundesverfassungsgerichts schon jetzt zu beachten.

15.5 Einführung eines Forschungsgeheimnisses für medizinische Daten

(Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004)

In vielen Bereichen der Forschung werden sensible medizinische Daten der Bürgerinnen und Bürger verarbeitet. Dabei ist häufig eine Verarbeitung auch personenbezogener Daten erforderlich. Diese Daten können mit Einwilligung der Betroffenen insbesondere von Ärztinnen und Ärzten, aber auch von Angehörigen anderer Heilberufe an Forscher und Forscherinnen übermittelt werden. Dies ist im Interesse der Forschung zwar grundsätzlich zu begrüßen. Mit der Übermittlung verlieren die Daten aber regelmäßig den strafrechtlichen Schutz vor Offenbarung und den Beschlagnahmeschutz im Strafverfahren. Auch ein Zeugnisverweigerungsrecht bezüglich dieser Daten steht den Forschenden - anders als insbesondere den behandelnden Ärztinnen und Ärzten - nicht zu. Zum Schutze der Forschung, vor allem aber zum Schutz der durch die Datenübermittlung und -verarbeitung Betroffenen, sollte vom Gesetzgeber deshalb sichergestellt werden, dass die bei den übermittelnden Stellen geschützten personenbezogenen medizinischen Daten auch nach ihrer Übermittlung zu Forschungszwecken den gleichen Schutz genießen.

Die Datenschutzbeauftragten fordern daher den Bundesgesetzgeber auf,

- in § 203 StGB die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,
- in §§ 53, 53 a StPO für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forscher und ihre Berufshelfer zu schaffen,
- in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten zu schaffen.

Die Datenschutzbeauftragten sehen in diesen Vorschlägen einen ersten Schritt zu einer generellen Regelung des besonderen Schutzes personenbezogener Daten in der Forschung.

15.6 Automatische Kfz-Kennzeichenerfassung durch die Polizei

(Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004)

Die Datenschutzbeauftragten des Bundes und der Länder betrachten einen anlassfreien und lageunabhängigen Einsatz von automatischen Kfz-Kennzeichen-Lesesystemen im Straßenverkehr mit Sorge, weil sich diese Maßnahmen zu einem weiteren Schritt zur Überwachung aller Bürgerinnen und Bürger entwickeln können.

Es ist zu befürchten, dass mit dem Einsatz der automatischen Kfz-Kennzeichenerfassung eine neue Infrastruktur geschaffen wird, die künftig noch weit tiefergehende Eingriffe in das Persönlichkeitsrecht ermöglicht.

Die Nutzung dieser neuen Technik hätte zur Folge, dass die Kfz-Kennzeichen aller an den Erfassungsgeräten vorbeifahrenden Verkehrsteilnehmerinnen und -teilnehmer erfasst und mit polizeilichen Fahndungsdateien abgeglichen würden. Schon der mit der Feststellung gesuchter Fahrzeuge verbundene Abgleich würde zu einem neuen Eingriff in das Recht auf informationelle Selbstbestimmung von Personen führen, die weit überwiegend keinen Anlass für eine polizeiliche Verarbeitung ihrer personenbezogenen Daten gegeben haben.

Auf jeden Fall muss ausgeschlossen werden, dass Daten über unverdächtige Personen gespeichert werden und dass ein allgemeiner Datenabgleich mit polizeilichen Informationssystemen durchgeführt wird.

Die Datenschutzbeauftragten weisen darauf hin, dass schon mehrere Länder eine Kfz-Kennzeichen-Erfassung ablehnen.

15.7 Gesetzentwurf der Bundesregierung zur Neuregelung der akustischen Wohnraumüberwachung

(Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. Oktober 2004)

Die Bundesregierung hat einen Gesetzentwurf zur Neuregelung der akustischen Wohnraumüberwachung vorgelegt. Sie setzt damit in großen Teilen das Urteil des Bundesverfassungsgerichts vom 3. März 2004 um, wonach die Vorschriften der Strafprozessordnung zum „großen Lauschangriff“ in wesentlichen Teilen verfassungswidrig sind. Allerdings sind zentrale Punkte, wie die Begriffsbestimmung des „unantastbaren Kernbereichs der privaten Lebensgestaltung“ und die Bestimmung des Kreises der Menschen „des persönlichen Vertrauens“ offen geblieben.

Ungeachtet dessen drohen im weiteren Verlauf des Gesetzgebungsverfahrens schwerwiegende Verschlechterungen: So wird diskutiert, die Vorgaben des Bundesverfassungsgerichts dadurch zu unterlaufen, dass auch bei erkannten Eingriffen in den absolut geschützten Kernbereich die technische Aufzeichnung fortgesetzt wird. Dies steht in eklatantem Widerspruch zur eindeutigen Vorgabe des Bundesverfassungsgerichts, die Aufzeichnung in derartigen Fällen sofort zu beenden. Darüber hinaus wird versucht, den Anwendungsbereich der akustischen Wohnraumüberwachung dadurch auszuweiten, dass auch nicht strafbare Vorbereitungshandlungen einbezogen werden. Auch dies widerspricht den verfassungsgerichtlichen Vorgaben und verwischt die Grenzen zwischen Strafverfolgung und Gefahrenabwehr.

Die Datenschutzbeauftragten bekräftigen im Übrigen ihre Forderung, dass es im Hinblick auf die Heimlichkeit der Überwachung und ihrer zwangsläufigen Berührung mit dem Kernbereich privater Lebensgestaltung erforderlich ist, alle Formen der verdeckten Datenerhebung an den Maßstäben der verfassungsgerichtlichen Entscheidung vom 3. März 2004 zu messen und auszurichten sowie die einschlägigen gesetzlichen Befugnisregelungen des Bundes und der Länder auf den Prüfstand zu stellen und gegebenenfalls neu zu fassen. Dies gilt etwa für die präventive Telekommunikationsüberwachung, die längerfristige Observation, den verdeckten Einsatz technischer Mittel, den Einsatz nachrichtendienstlicher Mittel und von verdeckten Ermittlern. Dabei sind insbesondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung und zum Schutz vertraulicher Kommunikation mit engsten Familienangehörigen und anderen engsten Vertrauten sowie mit Personen, die einem Berufsgeheimnis unterliegen, zur Einhaltung der Zweckbindung bei Weiterverwendung der durch die Eingriffsmaßnahmen erlangten Daten, zu der dazu erforderlichen Kennzeichnungspflicht und zur Benachrichtigung aller von der Eingriffsmaßnahme Betroffenen sowie zur detaillierten Ausgestaltung von Berichtspflichten gegenüber den Parlamenten vorzusehen.

15.8 Gravierende Datenschutzmängel bei Hartz IV

(Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. Oktober 2004)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass es bei der praktischen Umsetzung der Zusammenlegung von Arbeitslosen- und Sozialhilfe zu erheblichen datenschutzrechtlichen Mängeln gekommen ist. Diese bestehen sowohl bei den Verfahren der Datenerhebung durch die verwendeten Antragsformulare als auch bei der Leistungsberechnungs-Software (A2LL). Die Datenschutzdefizite wären vermeidbar gewesen, wenn datenschutzrechtliche Belange von Anfang an angemessen berücksichtigt und umgesetzt worden wären.

Zwar stellt die Bundesagentur für Arbeit (BA) seit dem 20. September 2004 sog. Ausfüllhinweise zum Antragsvordruck Arbeitslosengeld II zur Verfügung, in denen viele Bedenken der Datenschutzbeauftragten aufgegriffen werden. Allerdings ist hierbei zu berücksichtigen, dass durch die Ausfüllhinweise nicht mehr alle antragstellenden Personen erreicht werden können. Umso wichtiger ist es, dass die örtlich zuständigen Leistungsträger die verbindlichen Ausfüllhinweise beachten und die antragstellenden Personen, die ihren Antrag noch nicht eingereicht haben, vor der Abgabe auf diese hingewiesen werden. Personen, die ihren Antrag früher gestellt haben, dürfen nicht benachteiligt werden. Überschussinformationen, die vorhanden sind und weiterhin erhoben werden, sind zu löschen.

Darüber hinaus will die BA die in den Antragsformularen nachgewiesenen Datenschutzmängel in vielen Bereichen in der nächsten Druckauflage korrigieren und für das laufende Erhebungsverfahren zur Verfügung stellen. Gleichwohl ist zu befürchten, dass die Formulare nicht das erforderliche Datenschutzniveau erreichen.

Hinsichtlich der Software A2LL bestehen immer noch wesentliche Datenschutzmängel, die zu erheblichen Sicherheitsrisiken führen. Insbesondere besteht für die Sachbearbeitung ein uneingeschränkter bundesweiter Zugriff auf alle Daten, die im Rahmen von A2LL erfasst wurden, auch soweit diese Daten für die Sachbearbeitung nicht erforderlich sind. Dieser Mangel wird dadurch verschärft, dass noch nicht einmal eine Protokollierung der lesenden Zugriffe erfolgt und damit missbräuchliche Zugriffe nicht verfolgt werden können. Das Verfahren muss über ein klar definiertes Zugriffsberechtigungskonzept verfügen. Die Beschäftigten der zuständigen Leistungsträger dürfen nur den zur Aufgabenerfüllung erforderlichen Zugriff auf die Sozialdaten haben.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA auf, die notwendigen Schritte unverzüglich einzuleiten und nähere Auskunft über den Stand des Verfahrens zu erteilen.

15.9 Datensparsamkeit bei der Verwaltungsmodernisierung

(Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. Oktober 2004)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Bemühungen, Dienstleistungen der öffentlichen Verwaltung bürgernäher und effizienter zu erbringen. Sie fordern, dass im Zug von Maßnahmen der Verwaltungsreform die sich dadurch bietenden Möglichkeiten genutzt werden, um das Datenschutzniveau zu verbessern. Verwaltungsvereinfachung muss auch dazu genutzt werden, weniger personenbezogene Daten zu verarbeiten. Künftig müssen Verfahren und Datenflüsse wesentlich besser überschaubar und nachvollziehbar sein. Besonders sollen die Möglichkeiten der Technik genutzt werden, Risiken zu minimieren, die mit der Zentralisierung von Datenbeständen verbunden sind.

Werden Rechtsvorschriften, etwa im Steuerrecht oder im Arbeits- und Sozialrecht und hier insbesondere bei Änderungen in den Systemen der sozialen Sicherung, mit dem Ziel der Verwaltungsvereinfachung erlassen, sind die Auswirkungen auf den Datenschutz frühzeitig zu prüfen. Im Ergebnis müssen die Normen den gesetzlich verankerten Grundsatz der Datenvermeidung umsetzen und somit das Recht auf informationelle Selbstbestimmung gewährleisten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deswegen, bei Vorschlägen zur Verwaltungsvereinfachung und darüber hinaus bei allen Regelungsvorhaben darauf zu achten, dass das damit verbundene Potential an Datensparsamkeit und Transparenz ausgeschöpft wird.

Hierzu ist eine Folgenabschätzung auf mögliche Beeinträchtigungen der informationellen Selbstbestimmung vorzunehmen. Die Ergebnisse sind in geeigneter Form zu dokumentieren.

15.10 Staatliche Kontenkontrolle muss auf den Prüfstand!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Umlaufverfahren vom 26. November 2004)

Das „Gesetz zur Förderung der Steuerehrlichkeit“ vom 23. Dezember 2003 (BGBl. I 2003, S. 2928) enthält mit den §§ 93 Abs. 7, 8 und 93 b der Abgabenordnung Regelungen, die das Grundrecht auf informationelle Selbstbestimmung aller Bürgerinnen und Bürger im Bereich ihrer finanziellen und wirtschaftlichen Betätigung in erheblichem Maße beschränken. Die neuen Regelungen treten am 1. April 2005 in Kraft. Sie sehen vor, dass nicht nur Finanzbehörden, sondern auch eine unbestimmte Vielzahl weiterer Behörden Zugriff auf Bankdaten erhalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, diese Regelungen mit dem Ziel zu überarbeiten, das Recht auf informationelle Selbstbestimmung zu gewährleisten. Insbesondere das verfassungsrechtliche Gebot der Normenklarheit und die Transparenz des Verfahrens müssen beachtet werden.

Die Neuregelung erlaubt einen Zugriff auf Bankdaten, die von den Kreditinstituten bereits seit April 2003 zur Aufdeckung illegaler Finanztransaktionen vor allem zur Terrorismusbekämpfung nach § 24 c des Kreditwesengesetzes vorgehalten werden müssen. Dabei handelt es sich um die Kontenstammdaten der Bankkundinnen und Bankkunden und sonstigen Verfügungsberechtigten, wie z. B. Namen, Geburtsdaten, Kontonummern. Mit der neuen Regelung einher geht bereits eine von den Datenschutzbeauftragten des Bundes und der Länder im Gesetzgebungsverfahren Ende 2003 kritisierte Zweckänderung der Verwendung der von den Kreditinstituten vorzuhaltenden Daten.

Nunmehr sollen neben Finanzbehörden auch andere Behörden, z. B. die zahlreichen Stellen der Sozialleistungsträger, Auskunft erhalten, wenn die anfragende Behörde ein Gesetz anwendet, das „an Begriffe des Einkommensteuergesetzes“ anknüpft und eigene Ermittlungen dieser Behörde ihrer Versicherung nach nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Welche Behörden dies sein sollen, geht aus dem Gesetz nicht eindeutig hervor. Da das Einkommensteuerrecht eine Vielzahl von „Begriffen“ verwendet (neben den Begriffen „Einkommen“ und „Einkünfte“ etwa auch „Wohnung“, „Kindergeld“, „Arbeitnehmer“), ist wegen fehlender Begriffsbestimmungen nicht abschließend bestimmbar, welche Behörden die Auskunftsersuchen stellen dürfen. Dies jedoch ist nach dem verfassungsrechtlichen Bestimmtheitsgebot unverzichtbar. Zudem wird nicht deutlich, welche Zwecke ein Auskunftsersuchen rechtfertigen und nach welchen Regeln sie erfolgen sollen.

Von der Tatsache des Datenabrufs erfahren Kreditinstitute und Betroffene zunächst nichts. Die Betroffenen erhalten hiervon allenfalls bei einer Diskrepanz zwischen ihren Angaben (z. B. anlässlich Steuererklärung, BAföG-Antrag) und den Ergebnissen der Kontenabfragen Kenntnis, nicht jedoch bei einer Bestätigung ihrer Angaben durch die Kontenabfragen.

Die Auskunft erstreckt sich zwar nicht auf die Kontostände; auf Grund der durch den Abruf erlangten Erkenntnisse können jedoch in einem zweiten Schritt weitere Überprüfungen, dann auch im Hinblick auf die Guthaben direkt beim Kreditinstitut erfolgen.

Dass Betroffene von Abfragen, die zu keiner weiteren Überprüfung führen, nichts erfahren, widerspricht dem verfassungsrechtlichen Transparenzgebot. Danach sind sie von der Speicherung und über die Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Geschieht dies nicht, hat das zur Konsequenz, dass die Rechtsschutzgarantie des Art. 19 Abs. 4 Grundgesetz verletzt wird. Die Bürgerinnen und Bürger haben einen substantiellen Anspruch auf eine tatsächlich wirksame gerichtliche Kontrolle (s. Volkszählungsurteil, BVerfGE 65, 1, 70).

16. Anhang

16.1 Pressespiegel

Datum	Zeitung	Titel/Inhalt
01.01.2004	Weser-Kurier	**„Konkreter Verdacht nötig“** Datenschutzbeauftragter gegen flächendeckende Video-Erfassung
02.01.2004	Süddeutsche Zeitung	**Ein Staat mit tausend Augen** Die Ausweitung der Video-Überwachung folgt einer neuen Sicherheitslogik: Jeder ist verdächtig
03.01.2004	Bremer Nachrichten/ Weser-Kurier	**Datenschützer hilft Kampfhund-Haltern** Stadtamt muss keine Daten an Finanzämter herausgeben
06.01.2004	taz-nord-bremen	**Daumendrücken gegen Terror** US-Reisende mit einem Visum müssen einen Fingerabdruck abgeben und sich fotografieren lassen. Informationen werden zur Terrorismusbekämpfung mit Datenbanken abgeglichen
07.01.2004	Weser-Kurier	**Im Büro darf auch privat gesurft werden** Finanzressort erstellt Richtlinie zur Nutzung des Internets/„Bremen übernimmt Vorreiterrolle“
03.03.2004	Die Welt	**Bedenken gegen den Großen Lauschangriff**
03.03.2004	Der Spiegel online	**Großer Lauschangriff in weiten Teilen verfassungswidrig** Der große Lauschangriff ist zu erheblichen Teilen verfassungswidrig. Das Bundesverfassungsgericht in Karlsruhe verlangte in seinem heute verkündeten Urteil zahlreichen Nachbesserungen bis zum 30. Juni 2005.
04.03.2004	Delmenhorster Kreisblatt	**SPD und Grüne begrüßen Urteil** Lauschangriff „Bedenken bestätigt“
04.03.2004	Nordsee-Zeitung	**Neuer Streit um Lauschangriff**
04.03.2004	taz-nord-bremen	**SPD und Grüne: BVG-Urteil prima**
04.03.2004	Tagesspiegel Berlin online	**„Das Gesetz ändern“** Ministerin Zypries will auch die Telefonüberwachung prüfen
04.03.2004	Bremer Nachrichten/ Weser-Kurier	**Karlsruhe stopft Staat die Ohren** Großer Lauschangriff in Privatwohnungen nur noch stark eingeschränkt möglich
04.03.2004	Bremer Nachrichten/ Weser-Kurier	**„Menschenwürde hat Vorrang“** Der Bremer Richter Bernd Asbrock zum Urteil des Bundesverfassungsgerichts
04.03.2004	taz-nord-bremen	**Karlsruhe fängt Wanzen ein** Das Bundesverfassungsgericht erklärt den großen Lauschangriff für größtenteils verfassungswidrig. Jeder Bürger hat das Recht, in

		seiner Wohnung „in Ruhe gelassen zu werden“
04.03.2004	taz-nord-bremen	**Geständnisse am Küchentisch** Die Polizei darf Gespräche im „Kernbereich privater Lebensgestaltung“ nur mithören, wenn sie annehmen muss, dass übers Kriminelle gesprochen wird“.
15.03.2004	Die Welt	**Ringen um das neue Informationsfreiheitsgesetz** SPD will Paradigmenwechsel – CDU befürchtet Mehrbelastung für Behörden – Skepsis bei öffentlichen Gesellschaften
20.03.2004	Nordsee-Zeitung	**Café-Besuch mit Video-Überwachung** Landesdatenschützer legt Beschwerdebericht vor – Meldeamt patzt
20.03.2004	Weser-Kurier	**Daten von 17-Jährigen gingen vor Bremerhaven-Wahl an DVU** Landesbeauftragter listet Ärgernisse auf / Jahresbericht vorgestellt
20.03.2004	taz-nord-bremen	**Bedrohlicher Sammlertrick** Die Datensammlungen über Einzelpersonen werden größer. Damit bedroht die neue Sicherheitspolitik auch ein Grundrecht, wie Bremer Beispiele zeigen
20.03.2004	Die Welt-Bremen	**Datenschutzbeauftragter legt Jahresbericht vor**
20.03.2004	Kreiszeitung Syke	**P-Switch installiert** Datenschützer Sven Holst legt seinen Jahresbericht vor
20.03.2004	Delmenhorster Kreisblatt	**Schutzbedürfnis wird selbst zur Gefahr** Landesbeauftragter: Informationelle Selbstbestimmung immer stärker unter Druck
21.03.2004	Kurier am Sonntag	**„Datenbeauftragte fehlen in Behörden“**
04/2004	Bremborium	**Videoüberwachung in Bremen** Die Freiheit stirbt in kleinen Stücken
07.04.2004	Kreiszeitung Syke	**Von der Decke spähen die Kameras** Immer mehr Bahnen und Busse werden videoüberwacht
10.04.2004	Die Welt	**Rasterfahndung entwickelt sich zum Flop** Offenbar kein einziger Terrorist enttarnt
14.04.2004	taz-nord-bremen	**Luigi Controlletti braucht selbst Kontrolle** Personalüberprüfung von Schwarzfahrern geht ganz leicht
15.04.2004	taz-nord-bremen	**Kontrolleure sind keine Polizisten** Der Fall „Luigi Controletti”
15.04.2004	Süddeutsche Zeitung	**Nicht ohne einen Richter** Staatsanwaltschaft verweigert erstmals einen DNA-Massentest
15.04.2004	Nordsee-Zeitung	**DNA-Test: Entscheidung bis Montag**

17./18.04.2004	taz-nord-bremen	**Die Bremer Generalin bekommt für DNA-Massentest-Stopp jetzt Schützenhilfe vom Landesdatenschützer**
21.04.2004	BILD-Bremen	**Suche nach Vergewaltiger – DNA-Massentest genehmigt**
21.04.2004	Bremer Nachrichten/ Weser-Kurier	**DNA-Massentest in Bremerhaven genehmigt**
21.04.2004	Nordsee-Zeitung	**„Der nächste Schritt ist ein Speicheltest“** Gerichtsbeschluss erwirkt – nur noch freiwillig
21.04.2004	Delmenhorster Kreisblatt	**Nun DNA-Massentest bei Suche nach Vergewaltiger**
21.04.2004	taz-nord-bremen	**Massen-Gentest vorm Stapellauf** Staatsanwaltschaft befürwortet jetzt doch DNA-Massentest in Bremerhaven
22.04.2004	taz-nord-bremen	**Polizei gesteht Fehler ein** Bremer Polizei regelt Verfahren zur Identitätsprüfung mutmaßlicher Schwarzfahrer neu
01.05.2004	Nordsee-Zeitung	**„Speicheltests besser regeln“** Dringlichkeitsantrag von SPD und CDU an Senat
03.05.2004	Kreiszeitung Syke	**Eine sichere Grundlage** SPD fordert Regelung für Massentests
03.05.2004	Nordsee-Zeitung	**„DNA-Tests erleichtern“** Senator Thomas Röwekamp will Bremerhavener Fall in der Innenministerkonferenz diskutieren
12.05.2004	Bremer Nachrichten/ Weser-Kurier	**Spritze auch gegen Willen des Patienten** Sozialbehörde plant Gesetzesänderung bei psychisch kranken Gewalttätern / Bundesweite Vorreiterrolle
12.05.2004	taz-nord-bremen	**Handfeste Folgen eines Todesfalls** Bremens „Umgang mit gefährlich psychisch Kranken“ nimmt Formen an: Polizei erweitert Spektrum und informiert Zuständige
12.05.2004	Bremer Nachrichten/ Weser-Kurier	**Ausweitung von DNA-Tests?** Pro & Contra
13.05.2004	Bremer Nachrichten/ Weser-Kurier	**DNA-Massentest beginnt am Freitag** Polizei sucht gefährlichen Serientäter
14.05.2004	Bremer Nachrichten/ Weser-Kurier	**Mieter mit Sozialhilfe werden durchleuchtet** „Bremische fragt regelmäßig bei der Schufa nach
18.05.2004	Bremer Nachrichten/	**DNA-Test wird zum Flop**

	Weser-Kurier	1000 Männer ignorierten Aufruf
30.05.2004	Bremer Nachrichten/ Weser-Kurier	**Abkommen über Passagier-Daten**
30.05.2004	Welt am Sonntag	**Erstmals stehen die Kosten zur biometrischen Datenerfassung fest** Ausweise mit allen digitalen Merkmalen kosten über 600 Millionen Euro im Jahr
01.06.2004	taz nord bremen	**Passwort für Luigi Controllletti** Senat befasst sich mit Datenschutzverletzung: Der Polizei auf die Finger geschaut
03.06.2004	Bremer Nachrichten/ Weser-Kurier	**Bürgerschaft kurz und bündig** *Nummer sicher* Wer erhält am Telefon Auskunft über persönliche Daten von Fahrgästen?
03.06.2004	Die Welt	**Neuer DNA-Test frühestens im Herbst**
03.06.2004	Nordsee-Zeitung	**Neuer Speicheltest im Herbst**
03.06.2004	Kreiszeitung Syke	**DNA-Test erst im Herbst**
21.06.2004	Die Welt Bremen	**Rechtsausschuss am Mittwoch**
20.07.2004	Nordsee-Zeitung	**Scharfe Kritik an „Bürokratiemonster“** Anträge für das neue Arbeitslosengeld II sind auf dem Weg
20.07.2004	taz-nord-bremen	**Zündstoff Antragsformular**
20.07.2004	Kreiszeitung Syke	**Arbeitslose müssen Vermögen offen legen** Werte von Immobilien, Sparguthaben, Schmuck und Autos werden abgefragt
26.07.2004	BILD-Bremen	**Vorsicht Kamera!** In Bremen werden Straßen, Plätze und Gebäude rund um die Uhr gefilmt. BILD sagt Ihnen, wo Sie auf dem Bildschirm erscheinen
26.07.2004	taz-nord-bremen	**Sparsam beim Datensammeln**
31.07.2004	Kreiszeitung Syke	**Immer mehr Missbrauch mit EC-Karten** Bremer Polizei startet Projekt „Kuno“ zum Schutz von Einzelhändlern / Minutenschnelle Weitergabe der Daten
11.08.2004	Weser Report	**Einkaufen und selbst abrechnen** Erste vollautomatische Kasse Bremen steht bei real
21.08.2004	Kreiszeitung Syke	**CDU will mehr lauschen**
22.08.2004	Kurier am Sonntag	**Bürgers Bankdaten bald behördenoffen**
03.09.2004	Bremer Nachrichten/	**Röpke startet große Umfrage zur Gesundheit**

	Weser Kurier	In einem Fragenkatalog sollen 9.600 Bürger anonym Auskunft über Beratung und Versorgung geben
03.09.2004	taz-nord-bremen	**Der gläserne Patient** Eine Umfrage soll Sozialsenatorin Röpke helfen, gesundheitliche Vorsorge „effizienter“ zu gestalten
10.09.2004	taz-nord-bremen	**Abhör-Pläne vom Tisch** Zypries gibt im Streit um großen Lauschangriff nach. Berufsgeheimnisträger werden doch nicht abgehört.
10.09.2004	Bremer Nachrichten/ Weser Kurier	**Kein Lauschangriff auf Journalisten**
10.09.2004	taz-nord-bremen	**Kampf gegen Terror greift Bankgeheimnis an** Folge des 11. September: Um verdächtige Geldgeschäfte aufzuspüren, werden zahlreiche Privatkonten offen gelegt.
13.09.2004	Bremer Nachrichten/ Weser Kurier	**Probleme beim Online-Banking**
29.09.2004	Bremer Nachrichten/ Weser Kurier	**Promi-Kinder für Fotografen tabu**
07.10.2004	Stadtteil-Kurier	**Kameraüberwachung am Bahnhof?** Streit um Rampe und Fahrstuhl / Oslebshausen bleibt im Blickfeld der Kommunalpolitik
20.10.2004	Bremer Nachrichten/ Weser Kurier	**Bremen möchte ganz vorne mit dabei sein** Bewerbung als Testregion für Gesundheitskarte
20.10.2004	Die Welt	**Bremen will elektronische Gesundheitskarte testen** Hansestadt bewirbt sich als Modellregion – Verwaltung. Ärzte und Krankenkassen arbeiten eng zusammen
20.10.2004	Delmenhorster Kreisblatt	**Bremen strebt Vorreiterrolle an** Stadt will zur Modellregion für die neue Gesundheitskarte werden
20.10.2004	Nordsee-Zeitung	**„Der gläserne Patient wird nicht kommen“** Bremen will Testregion für Gesundheitskarte werden – Datenschutz noch nicht gesichert
20.10.2004	Kreiszeitung Syke	**Alle Partner an einem Tisch** Bremen bewirbt sich als Testregion für die „elektronische Gesundheitskarte“
20.10.2004	taz-nord-bremen	**Röpke will Gesundheitskarte**
31.10.2004	Weser-Report	**Wut auf GEZ-Mitarbeiter** Rigoroses Vorgehen treibt Internatsbewohner auf die Barrikaden
05.11.2004	Bremer Nachrichten/ Weser Kurier	**Grüne bleiben bei Nein zu Kameras** Güldner: Statistik belegt Erfolge nicht

17.11.2004	Weser-Report	**Werden bald alle ausspioniert?**
		Datenschützer warnt in der Entwicklung zu mehr Videoüberwachung vor Gleichgültigkeit
25.11.2004	Nordsee-Zeitung	**Als Pleitegeier für immer geächtet?**
		Datenschützer bemängeln Anzeige im Internet
25.11.2004	taz-nord-bremen	**Positive Bilanz**
		Wenig Kritik am Datenschutz der bremischen Verwaltung
15.12.2004	Nordsee-Zeitung	**DNA-Reihentest: 2.399 Männer sind unverdächtig**
		Noch 46 „offene Posten“ gibt es in der Kripo-Statistik – Erste Vernehmungen bei der Staatsanwaltschaft
22.12.2004	Nordsee-Zeitung	**Datenschutz gilt auch für Jugendliche**
22.12.2004	Kreiszeitung Syke	**Datenschutz spielend lernen**
22.12.2004	Bremer Nachrichten/ Weser Kurier	**Schutz für Schüler beim Surfen im Internet**
		Datenschutzbeauftragter informiert junge Menschen jetzt online
12/2004	STERN	**Insolvenzen – für immer gebrandmarkt?**

16.2 Auswahl telefonisch beantworteter Anfragen

Thema	Anfragesteller/in
Weitergabe von Daten über Arbeitseinschränkungen an den Dienstherrn durch den amtsärztlichen Dienst	Beamter
Weitergabe von Beschäftigtendaten an die Agentur für Arbeit durch eine Verleihfirma	Arbeitsloser
Veröffentlichung von Gutachterdaten der Handwerkskammer durch Dritte	Handwerkskammer
Voraussetzung für die Bestellung eines betrieblichen Datenschutzbeauftragten	potenzieller betrieblicher Datenschutzbeauftragter
Nutzung von Diskussionsforen aus dem Internet für ein Forschungsprojekt	Hochschule
Meldepflicht bei Kundenbindungsprogrammen	Datenschutzbeauftragte
Datenschutz im Copyshop	Bürgerin
Private Bankverbindung bei der Bestellung von Musicalkarten	Bürgerin
Bürger erhält unerwünschte Werbung. Was kann man dagegen tun?	Bürger
Wie kann ich es verhindern, dass meine Adresse weitergegeben wird?	Bürger
War es zulässig, meine Adresse weiterzugeben?	Bürgerin
Durch Krankheit des Ehemannes wurde die Reiserücktrittsversicherung in Anspruch genommen. Sind Fragen und Schweigepflichtentbindung okay?	Bürgerin
Unterstützungsunterschriften für die Landtagswahl. Ist dies rechtens (Verbot des Ausforschens)?	Parteibüro
Darf die Sparkasse bei Bezahlung per Lastschrift Adresse an das Kaufhaus weitergeben, weil ein Restbetrag fehlt?	Bürger
Darf der Betriebsrat regelmäßig über Fehlzeitengespräche zwischen Vorgesetztem und Mitarbeiter informiert werden?	Beschäftigte
Darf die Polizei in pol. Auskunftssystem nach Straftaten von Polizeibewerbern fragen?	Polizeibewerber
Darf die Bauordnungsbehörde sich bei Nachbarn in Kleingärten Informationen über die Nutzung von Kleingärten holen?	Parzellenbesitzer
Kontrolle und Überwachung von Mitarbeitern hinsichtlich privater und dienstlicher Telefonate, E-Mails und Internet.	Unternehmen
Wann werden Daten bei der Polizei gelöscht. Löschung von "Jugendsünden" bei Einstellung in einem Wachunternehmen	Wachmann
Fragen nach dem Überprüfungsverfahren bei Luftpersonal (Flughafen). Der Anrufer erhielt Hinweise auf Fundstellen	Rechtsanwalt
Schufa-Einverständniserklärung bei Guthaben-Konto	Bankkunde
Speicherung von Gesundheitsdaten über Arbeitnehmer im öffentlichen Ordner eines Betriebes	Betriebsrat
Creditreform-Auskunft an Makler; falsche Auskunft wg. Namensgleichheit	Mietinteressent
Bekanntgabe von Bewerberdaten	Hochschullehrer
Erteilung unrichtiger Auskünfte durch Creditreform Bremen	Privatperson
Darf die Hausverwaltung einen an sie gerichteten Brief einfach kopieren und an die Bewohner/Eigentümer weitergeben?	WE-Eigentümer
Fragebogen einer Krankenkasse im Zusammenhang mit der Beantragung einer Kur	Versicherter
Zugang zu Aktenvernichtungstonnen	Mitarbeiter

Thema	Anfragesteller/in
Speicherung von Daten im Polizeicomputer	Bürger
Dürfen Ärzte Laborwerte aller Patienten in einem Krankenhaus einsehen?	Arzt
Angebot für eine Trauerfallversicherung, kann sich nicht erklären, woher Kaufhaus ihre persönlichen Daten einschließlich Geburtsdatum hat.	Bürgerin
Dürfen Administratoren von Mail-Servern abgesendete Mails lesen?	Bürger
Zum Thema Mammascreening	Bürgerin
Unternehmer möchte Online-Schulungen anbieten. Sein Partnerunternehmen ist in den USA ansässig.	Unternehmer
Datenspeicherung bei Auskunftei	Unternehmen
Negative Schufa-Auskunft	Bürgerin
Heimbewohnerin wendet sich gegen Vorenthalten ihrer Post durch Betreuerin	Bürgerin
Unzulässige Daten auf Krankenversichertenkarte	Bürgerin
Darf ein Notar in einer Teilungserklärung allen Miteigentümern die Geburtsdaten, die Grundschuld- und Hypothekengläubiger offenbaren?	Miteigentümer
Geldautomat Videoüberwachung	Bankkunde
Übermittlung von Spendernamen und Summen durch Empfänger an Spendensammler	ehrenamtlicher Mitarbeiter
Mitteilung der Justiz an das AfSD über drohende Obdachlosigkeit/Personenverwechslung	Bürgerin
Auskunft des Bundesamtes für Finanzen an Sozialamt/Freistellungsaufträge	Bürger
Angaben persönlicher Daten bei Einkauf	Bürger
Auskunft von GEZ-Daten	Bürger
Bekanntgabe von Stellenplan an Delegiertenversammlung	Kammer
Einsichtnahme in Patientenakte durch Doktorandin	betrieblicher Datenschutzbeauftragter
Übermittlung von Klientendaten aus Wohnheim für Suchtkranke an SPsD	Anfrage des Wohnheims
Kennzeichnung von Akten von Patienten mit Infektionskrankheiten	Krankenhaus
Löschungsfristen bei Auskunftei	Bürger
Datenerhebung durch Telekommunikations-Diensteanbieter bei Abschluss eines Telekommunikationsvertrages	Bürger
Verlangen des AfSD, Ärzte von ihren Schweigepflichten zu entbinden	Empfänger von Sozialhilfe/ Grundsicherung
Adressweitergabe für Gewinnspiele	Bürgerin
Verletzung von Persönlichkeitsrechten durch die Presse	öffentliche Einrichtung
Kundenkartei bei Unternehmensverkauf	Kundin
Befragung von Privathaushalten zum Zwecke des Adresshandels	Bürger
Falsche Zustellung durch Briefträger	Adressat
Zugriff auf Krankenakte aus psychiatrischer Behandlung im Krankenhaus	Patient
Faxirrläufer - Röntgenbericht von Arztpraxis erhalten	Privatperson
Postöffnung durch Insolvenzverwalter	Bürger
Anforderung von ESt-Steuerbescheid durch AOK zwecks Beitragsberechnung	Freiwillig Versicherter
Meldung von Arzt an Arbeitgeber über Arbeitsfähigkeit	Patient
Umgang mit den Daten von Krankenhausmitarbeitern mit ansteckenden Infektionen	Ärzte, Pflegekräfte
Datenaustausch zwischen Jugendämtern Syke und Bremen	Unterhaltsverpflichteter

Thema	Anfragesteller/in
Insolvenzdaten bei der Schufa	Kontoinhaber
Internes Bankgeheimnis	Kreditnehmerin
Foto-Aufnahmen von Besuchern des Zoos Hannover	Besucherin aus Bremen
Bekanntgabe des Gutachtens einer Familienhelferin im Sorgerechtsverfahren an Vater	Bürgerin
Identitätsfeststellung bei Kontoeröffnung	Bankkunde
Darf die Führerscheinstelle die Herausgabe einer Akte an Betroffene zur Weitergabe an den behandelnden Arzt im Rahmen der Fahrtauglichkeitsprüfung ablehnen?	Patientin
Schufa-Eintrag, Konto in Abwicklung	Bankkundin
Darf das Sozialamt die Vorlage eines Kontoauszugs verlangen, bei dem die Namen einzelner Empfänger kleinerer Beträge nicht geschwärzt sind?	Sozialhilfe Beantragende
Negative Schufa-Eintragung, Löschungsfrist	Bankkunde
Datenerhebung bei Anzeigenaufgabe von Zeitungen	Bürgerin
Schutz vor Dialern	Firma
Schufa, fehlerhafte Daten	Bankkunde
AOK fordert Einkommenssteuerbescheid von freiwillig Versicherten für Beitragsberechnung	Versicherter
Daten aus Testament	Bürger
Rechtsfolgen bei unerlaubter Versendung von MMS	Bürger
Schufa, Datenspeicherung	Bankkunde
Anschriften Direktmarketing	Bürger
Kundendaten-Übermittlung durch Autohändler an Hersteller	Kunde
Auslegung von datenschutzrechtlichen Vertragsklauseln, Datenübermittlungen innerhalb Europas	Pharma-Firma
Zulässigkeit von Videoüberwachungen in der Straßenbahn	Bürger
Speicherung von Kundendaten durch Handelsunternehmen	Kunde
Angabe der Schulausbildung bei Beantragung von Sozialhilfe	Bürgerin
Bekanntgabe der Telefondurchwahl einer Krankenhauspatientin	Bürgerin
Vorlage von Kontoauszügen beim Sozialamt	Bürgerin
Geheimhaltungspflicht der Mitarbeiter bzgl. Gesundheitsdaten	Pflegedienst
Erteilung von Auskünften durch Creditreform	Bürgerin
Auskunftei, Datenübermittlung in das Ausland	Bürgerin
Datenerhebung durch Kreditinstitut	Bürger
Bestellung eines betrieblichen Datenschutzbeauftragten	Fotounternehmen
Erteilung von Auskünften durch Auskunfteien	Bürger
Datenübermittlung an die GEZ	Bürger
Datenschutz bei Erbschaftssachen	Bürger
Weitergabe von Daten an Unternehmen	Bürger
Datenübermittlung an die GEZ	Bürger
Veröffentlichung personenbezogener Daten auf Internetseiten	Wohnungsbaugesellschaft
Versand von Botenpost (Vertraulichkeit)	Mitarbeiterin
Datenübermittlung in die USA, Safe-Harbor, Codes of Conduct	Unternehmen
Konsequenzen für Patienten bei Einführung des eRezepts	Bürger
Bestellung eines behördlichen Datenschutzbeauftragten	Behörde
Erhebung von Daten beim Mikrozensus 2004	Bürger

Datenverarbeitung durch Kreditinstitut	Bürgerin
Thema	**Anfragesteller/in**
Erteilung von Auskünften durch Creditreform	Bürger
Weitergabe von Daten eines Versicherungsmaklers durch eine Versicherung	Bürger
Speicherung von Daten durch Creditreform	Bürger
Bestellung eines betrieblichen Datenschutzbeauftragten	Handelsunternehmen
Überprüfung der privaten Handy-Nutzung durch den Arbeitgeber	Geschäftsführer
Führung des Verfahrensverzeichnisses	Unternehmen
Videoüberwachung in einer Umkleidekabine eines Kaufhauses	Kunden
Vervielfältigung eines Fotos (Copyright, Datenschutz)	Bürger
Zulässigkeit der automatisierten Verarbeitung von Personaldaten	Arbeitnehmer
Weitergabe von E-Mails an Strafverfolgungsbehörden	Provider
Widerspruch gegen die Datenübermittlung durch die Stadtwerke	Stalking-Opfer
Übermittlung von Daten in die USA, Codes of Conduct	Arbeitnehmerkammer
Veröffentlichung von Sponsoren in einer Zeitung	Zeitung
Abmahnungsschreiben auf dem Schreibtisch einer anderen Kollegin	Arbeitnehmerin
Fragebogenaktion des Betriebsrats zur Gesundheit, Zusammenarbeit mit Vorgesetzen und zum Betriebsklima	Arbeitnehmer
Übermittlung von Meldedaten an die GEZ	Bürger
Übermittlung von Daten an die GEZ	Bürger
Umfang der Kontrolle der Arbeitnehmer bei technischen Arbeiten durch den Arbeitgeber	Arbeitnehmer
Durchführung des Mikrozensus	Bürgerin
Zulässigkeit der Übermittlung von Arbeitnehmerdaten an eine Stelle in Singapur	Arbeitnehmer
Fragenbogenaktion im Vorfeld eines Internet-Shops	Selbständiger
Übermittlung von Arbeitnehmerdaten in die USA	Arbeitnehmer
Meldungen bei Datenübermittlungen an die Kommission	Lebensmittelunternehmen
Kundenbefragung, anonymisierte Erhebung von Daten, Einwilligung	Selbständiger
Beschlagnahme von Patientendaten bei einem Physiotherapeuten	Physiotherapeut
Auskunft wegen Datenerhebungsumfang bei Bonitätsprüfung nach dem Ausländergesetz	Bürger
Datenübermittlung in Drittstaaten: Betriebsvereinbarung, Einwilligung, Standardverträge und Genehmigungspflicht	Kammer
Veröffentlichung von Bewerberprofilen im Internet als Bewerberbörse durch Arbeitsvermittler	Arbeitnehmer
Regelmäßige Datenübermittlung zwischen Meldeamt und Amt für Bauförderung zur Prüfung der berechtigten Belegung von Sozialwohnungen	Berechtigungsschein-inhaber
Bestellung eines betrieblichen Datenschutzbeauftragten, Voraussetzungen	Hotel
Videoüberwachung durch den Nachbarn	Wohnungsinhaber
Verdacht der unzulässigen Datenverarbeitung durch den getrenntlebenden Partner	Arbeitnehmer
Anbringung einer Tafel über Pflegeheimbewohner und diese betreuenden Beschäftigten in Personalzimmern des Pflegeheimes	Heimbewohner
Bestellung des betrieblichen Datenschutzbeauftragten	EDV-Unternehmen
Verwendung von Videoaufzeichnung in eine Wohnanlage für künstlerische Zwecke	Bewohner

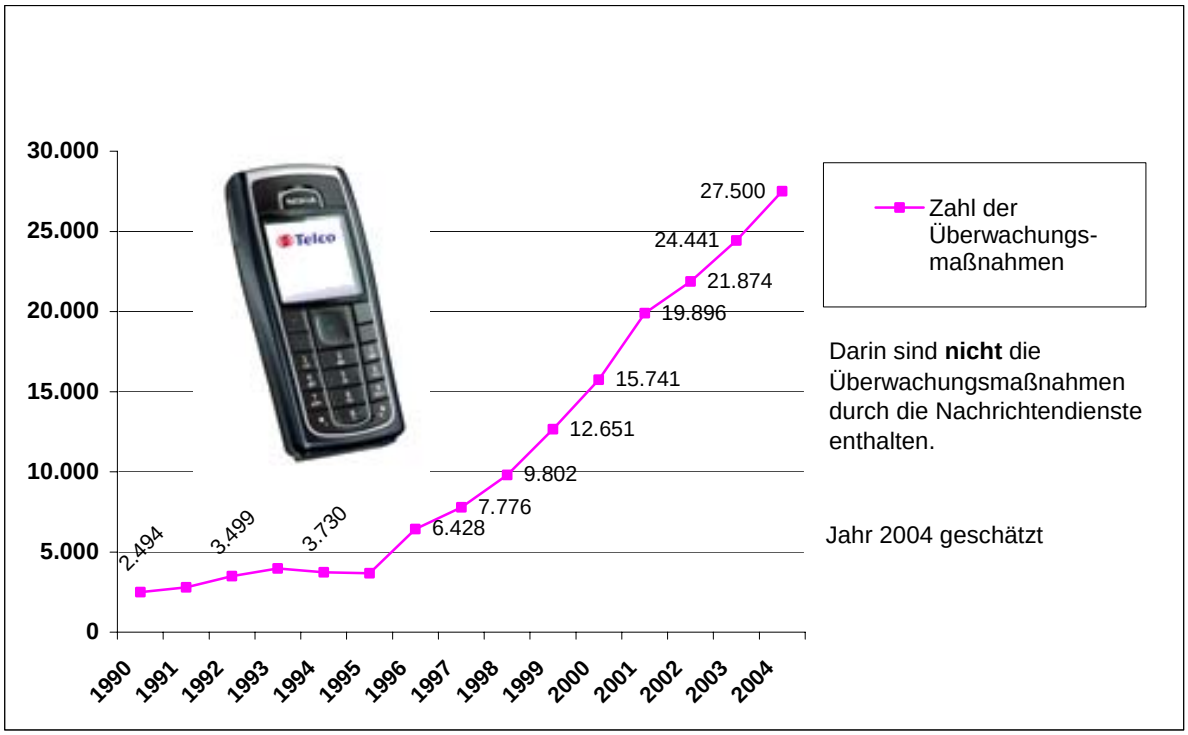
Offenbarung von Personaldaten durch Presseerklärung	Unternehmer

Thema	**Anfragesteller/in**
Datenübermittlung in die USA, Safe-Harbor, Codes of Conduct, verbindliche Unternehmensregelungen, Verfahren bei der Genehmigung von verbindlichen Unternehmensregelungen	Unternehmensverband
Vernichtung von Forschungsunterlagen	Wissenschaftlerin
Anforderungen an den betrieblichen Datenschutzbeauftragten	Bürger
Weitergabe von gesundheitlichen Daten eines Arbeitnehmers im Rahmen eines Arbeitsgerichtsprozesses an Arbeitgeber und Kollegen	Arbeitnehmer
Bestellung eines betrieblichen Datenschutzbeauftragten wg. Verarbeitung von Gesundheitsdaten	Mitglieder eines Vereins
Stalking: Wie kann man sich gegen Verfolgung wehren?	Bürgerin
Offenbarung von Sozialdaten im Gerichtsverfahren	Sozialleistungsempfänger
Hilfestellung beim Ausfüllen der ALG-II-Formulare	potentieller ALG-II-Empfänger
Bestellungspflicht für Rechtsanwaltskanzlei und Notariat von Datenschutzbeauftragten, Zulässigkeit von externen Datenschutzbeauftragten, Berufsgeheimnisträger	Rechtsanwälte
Übermittlung durch Auskunftei	Bürgerin
Forderung über fällige Lohnkosten per Postkarte durch einen ehemaligen Arbeitnehmer	Arbeitgeberin
Bestellung betrieblicher Datenschutzbeauftragter durch Steuerberater	Unternehmen
Umgang mit online übermittelten Bewerbungsdaten	Bewerber
Adressierung von Vollstreckungsverfahren durch Finanzamt	Vollstreckungsschuldner
Auskunftsersuchen an die Polizei	Bürger
Auskunftsersuchen wegen Lifestyle-Umfrage	Bürgerin
Veröffentlichung von fünfzig Jahre alten Daten	Bürger
Auskünfte der Einwohnermeldebehörde	Bürgerin
Videoüberwachung eines Privatweges	Bewohner
Zulässigkeit von Kundenbindungssystemen	betrieblicher Datenschutz-beauftragter
Weitergabe von Stellenbeurteilungen	Beschäftigte
Weitergabe der Verbrauchsdaten an alle Eigentümer einer Wohnanlage	Wohnungseigentümer
Anonymisierung der Eltern- und Schülerdaten bei Forschungsvorhaben in Schulen	Eltern und Schüler
Psychologische Tests im Bewerbungsverfahren	Bewerber
Datenlöschung bei Kreditinstituten	Bürgerin
Rechner wird durch Portscans massiv frequentiert. Ist das zulässig? Was kann man tun?	Bürger
Fragen zur Datenübermittlung zwecks Abrechnung von Schornsteinfegergebühren	Bürger
Möglichkeit der Bestellung eines betrieblichen Konzernbeauftragten	Unternehmen
Fragen zur Gebäudeversicherung im Antrag auf eine KfZ-Versicherung	Bürger
Datenübermittlung der Schufa	Bürgerin
Weitergabe von Insolvenzdaten an die Schufa	Bürger
Fragen zur Datenerhebung durch Marktforschungsinstitut	Bürger
Fragen zu SMS-Spams	Bürger

Frage zu Dialern bei Telefonie	Bürger

Thema	**Anfragesteller/in**
Persönliche Daten (z. B. Rentenversicherungsnummer) sichtbar im Fenster eines Briefumschlages der Bundesagentur für Arbeit	Arbeitssuchende
Löschungsfristen bei Auskunfteien	Bürger
Datenübermittlungen von Creditreform Bremen	Bürgerin
Adressankauf durch GEZ	Bürgerin
Frage zu Berufsunfähigkeitsversicherung	Bürger
Angabe von Gründen bei Abmeldung bei der GEZ	Bürger
Datenerhebung für Wirtschaftsstatistik	Bürger
Zulässigkeit der Weitergabe von Daten von der JVA an das Gericht	Journalist
Beobachtet eine Polizei-Kamera meine Wohnung?	Bürger
Weitergabe von personenbezogenen Daten durch Insolvenzverwalter	Bürger
Biometrische Daten in Reisepässen	Bürgerin
Umgang mit Spamfaxen	Bürger
Bekanntgabe von Mitgliederdaten eines Vereins	Bürgerin

16.3 Anstieg der Telefonüberwachung



16.4 Liste des verfügbaren Informationsmaterials

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

Folgende Informationsmaterialien können beim

Landesbeauftragten für den Datenschutz der Freien Hansestadt Bremen
Postfach 10 03 80, 27503 Bremerhaven
Telefon: 04 71/9 24 61-0
Telefax: 04 71/9 24 61-31
E-Mail: office@datenschutz.bremen.de
angefordert werden:

24. Jahresbericht 2001, Bürgerschafts-Drs. 15/1106		(Restexemplare)
25. Jahresbericht 2002, Bürgerschafts-Drs. 15/1418		(Restexemplare)
26. Jahresbericht 2003, Bürgerschafts-Drs. 16/189		(Restexemplare)

Broschüre	„Mobilfunk und Datenschutz"
Broschüre	„Datenschutz bei WindowsNT"
Broschüre	„Handlungsempfehlungen datenschutzgerechtes e-Government“
Faltblatt	„Datenschutz im Verein“
Faltblatt	„Adressenhandel und unerwünschte Werbung"
Faltblatt	„Handels- und Wirtschaftsauskunfteien"
Faltblatt	„Hinweise zum Antrag Arbeitslosengeld II“
Faltblatt	„Meine Datenschutzrechte als Telefonkunde“
Faltblatt	„Keine Spione auf der Festplatte“
Faltblatt	„Verräterische Spuren auf Festplatten“
BfD–Info 1	Bundesdatenschutzgesetz - Text und Erläuterungen -
BfD–Info 2	Der Bürger und seine Daten
BfD–Info 3	Schutz der Sozialdaten
BfD–Info 4	Die Datenschutzbeauftragten in Behörde und Betrieb
BfD–Info 5	Datenschutz in der Telekommunikation

16.5 Glossar

Abkürzung	Erklärung
A2LL	Verfahren zur Berechnung des Arbeitslosengeldes II
ABMG	Autobahnmautgesetz für schwere Nutzfahrzeuge
Access-Point	Übergabepunkt vom Funkbereich zum Netz
AFIS	Automatisierters Fingerabdruck-System
AFZ	Ausbildungsförderungszentrum im Land Bremen GmbH
ALG II	Arbeitslosengeld II
AO	Abgabenordnung
Auditing	Gutachterliche Untersuchung eines DV-Verfahrens
Authentifizierung	Ausweisen für einen berechtigten Zugriff
BA	Bundesagentur für Arbeit
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Datenschutz
BIPS	Bremer Institut für Präventionsforschung und Sozialmedizin
BKA	Bundeskriminalamt
BMWA	Bundesministerium für Wirtschaft und Arbeit
BreKom	Bremer Kommunikationstechnik
BremDSG	Bremisches Datenschutzgesetz
BremPolG	Bremisches Polizeigesetz
BVerfG	Bundesverfassungsgericht
BVN	Bremer Verwaltungsnetz
BZRG	Bundeszentralregistergesetz
Client	Beteiligung eines PC (Kunde) in einem Netzwerk
Dakota	Datenaustausch und Kommunikation auf Basis Technischer Anlagen
DV	Datenverarbeitung
eGovernment	elektronische Verwaltung
ELSTER	Elektronische Steuererklärung
EU	Europäische Union
EVGP	Elektronisches Verwaltungs- und Gerichtspostfach
FEBB	Freie Evangelische Bekenntnisschule Bremen
Firewall	Programm zum Schutz von Angriffen aus dem Internet
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz
GKV	Gesetzliche Krankenversicherung
GPS	Global Positioning System
GSM	Mobiltelefonstandard
HNO-Ärzte	Hals-Nasen-Ohren-Ärzte
Homepage	Eingangs- und Eröffnungsseite einer Internetadresse
iBON	integratives Bremer Onkologie- und Hämatologie Netzwerk
InsO	Insolvenzordnung
IPSec	Internet Protocol Security
ISA	Informationssystem Sachen und Anzeigen
ISDN	Integrated Services Digital Network (das digitale Telefonnetz)
KUNO	Kriminalitätsbekämpfung im unmittelbaren Zahlungverkehr unter Nutzung nichtpolizeilicher Organisationsstrukturen
KWG	Kreditwesengesetz

Abkürzung	Erklärung
LAN	Local Area Network (lokales Netzwerk)
MiP	Mitarbeiterportal
MiStra	Anordnungen über Mitteilungen in Strafsachen
Monitoring	Überwachung während des laufenden Betriebs
NADIS	Nachrichtendienstliches Informationssystem
OBU	On-Board Unit
PAT	Programm zur Auswertung von Telekommunikationsüberwachungen
PDA	Personal Digital Assistant (elektronisches Notizbuch)
PKI	Public Key Infrastructure
PROHEIM	Programmierte Heimhilfe
PROSOZ	Programmierte Sozialhilfe
PuMa	Personalverwaltung und -management
Router	Gerät, zum Steuern von Datenpaketen im Netz
Security-Gateway	Rechner, der Daten- bzw.Rechnernetze sicher verbindet
Server	ist ein Computer in einem Netzwerk, der andere Computer bedient
Signatur	elektronische Unterschrift
Slotmachine	Spielautomat
SOLAS	Safety of Life at Sea
SSH	Secure Shell (Protokoll, das sichere Verbindungen in unsicheren Netzen gestattet)
SSID	Service-Set-Identifier (Name eines WLNA-Dienstenetzes)
SSL	Security Socket Layer (Internet-Protokoll zur sicheren Datenübertragung)
StPO	Strafprozessordnung
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
USB	Universal Serial Bus, standartisierte Steckverbindung
VERA	Vergleichsarbeiten an Bremer Schulen
VHS	Volkshochschule
VPN	Virtual Private Network
VPN-Tunnel	Virtual Privat Networking, abgesicherter Datenstrom
VPS	Virtuelle Poststelle
WLAN	Wireless Local Area Network (Funknetz)
X.509-Zertifikat	Internationaler Zertifikate-Standard
ZSS	Zentrale Speicherstelle

16.6 Index