20. Tätigkeitsbericht
des
Hamburgischen Datenschutzbeauftragten
zugleich
Tätigkeitsbericht der Aufsichtsbehörde
für den nicht öffentlichen Bereich
2004 / 2005

vorgelegt im März 2006

Hartmut Lubomierski
(Redaktionsschluss: 31. Dezember 2005)

Diesen Tätigkeitsbericht können Sie abrufen unter
www.datenschutz.hamburg.de

Herausgegeben vom Hamburgischen Datenschutzbeauftragten
Klosterwall 6 (Block C) · 20095 Hamburg · Tel. 428 54 40 40 · Fax 428 54 40 00
mailbox@datenschutz.hamburg.de

Auflage: 1.500 Exemplare

Druck: Lütcke & Wulff, 20097 Hamburg

INHALTSVERZEICHNIS

DATENSCHUTZ IM ÖFFENTLICHEN BEREICH

DATENSCHUTZ IM NICHT-ÖFFENTLICHEN BEREICH

BÜRGERSERVICE UND DIENSTSTELLE

Vorbemerkung

Nicht: „Ich denke, also bin ich." gilt unter den Funktionsbedingungen der Informationsgesellschaft und der Konsumgesellschaft, in der wir leben, sondern: „Ich kommuniziere, also bin ich." und „Ich konsumiere, also bin ich."

Für den Staat und seine Sicherheitsbehörden ist daraus geworden: „Ich kommuniziere, also bin ich potentiell verdächtig." Also wird mein Kommunikationsverhalten erfasst und gespeichert. Für die Wirtschaft und ihre Marketingstrategen ist daraus geworden: „Ich konsumiere, also bin ich ein potentieller Kunde." Also wird mein Konsumentenverhalten erfasst und gespeichert und ausgewertet.

Dabei ist die fast vollständige elektronische Erfassung und Speicherung aller Kommunikations- und Konsumentendaten für Staat und Wirtschaft so verführerisch einfach geworden, dass ihr kaum etwa entgegenzusetzen ist, weil sie unter zwei Bedingungen erfolgt, die es bisher so noch nicht gegeben hat:

Noch nie zuvor wurde unser Kommunikations- und unser Konsumverhalten so extrem elektronisch unterstützt und konnte technisch so perfekt und eindeutig abgebildet und aufgezeichnet und gespeichert werden wie heute.

Briefe schreiben ist aus der Übung und aus der Mode gekommen. Wir kommunizieren am Arbeitsplatz wie auch privat ganz überwiegend elektronisch vermittelt über Telefon, Handy, E-Mail und Internet. Alle bei diesen Kommunikationsformen anfallenden Verbindungsdaten werden heute bereits lückenlos elektronisch erfasst und gespeichert. Und sie sollen künftig europaweit für mindestens sechs Monate auf Vorrat gespeichert werden. Wir bezahlen immer weniger unregistriert mit Bargeld. Wir kaufen immer häufiger personalisiert per Bankkarte, Kundenkarte, Kreditkarte, wir bestellen per Internet, buchen online. Unser Kaufverhalten wird dadurch elektronisch erfasst und gespeichert.

Die Vorstellung, diese immense Flut von Daten könne weder von Seiten des Staates noch von Seiten der Wirtschaft sinnvoll verwaltet werden, es würden lediglich riesige „Datenfriedhöfe" angesammelt, deren Auswertung jede Kapazität sprengen würde, ist überholt. Die Speicherung und Verarbeitung dieser Datenmengen bereitet heute keine wesentlichen technischen Schwierigkeiten mehr. Die Speicherkapazitäten sind vorhanden und wirtschaftlich zu betreiben. Die Schufa verfügt über 360 Millionen Informationen zu über 62 Millionen Personen. Jede Nacht werden die Daten von über zweihundertfünfzig Millionen Konten übermittelt. Auf die Suchmaschine Google, die über 8 Milliarden Webseiten auswertet und eine Milliarde Bilder bereithält, erfolgen täglich mehrere hundert Millionen Zugriffe. Das System ist so ausgelegt, dass die Kapazitäten mit geringem Aufwand nahezu grenzenlos erweitert werden können.

Aber die elektronische Erfassung des Menschen geht noch viel weiter. Unser Bewegungsverhalten im öffentlichen Raum und in der Freizeit wird vielfältig

beobachtet und ist weitgehend nachvollziehbar, denn jedes Handy wird automatisch geortet, im öffentlichen Raum und im Einkaufszentrum findet Videoüberwachung statt, auf den Autobahnen erfolgt die Fahrzeugregistrierung per Toll Collect und die automatische Kennzeichenerfassung, mit der RFID-Technologie kommt die automatische Zutritts- und Bewegungserfassung. Die Gehaltsdaten aller Beschäftigten in Deutschland sollen im Rahmen des JobCard-Verfahrens in einem Zentralregister gespeichert werden. Unsere Identität wird biometrisch erfasst und gespeichert in biometrischen Passdaten. Unsere genetische Disposition wird durch Gentests immer vorhersagesicherer feststellbar. Es werden Tests entwickelt, die Aussagen über Lebenserwartung, Eigenschaften, Leistungsfähigkeiten sowie Veranlagungen zu Krankheiten ermöglichen. Körperliche Spuren wie Haare, Speichelreste, die wir hinterlassen, sind anhand des DNA-Identifikationsmusters uns eindeutig zuzuordnen. Stichwort: Genetischer Fingerabdruck.

Nehmen wir alle diese Daten zusammen, die von uns erfasst werden, so ergibt sich ein Befund, auf den die Metapher „gläserner Mensch“ zutrifft.

Heute gilt wie nie zuvor: „Ich werde erfasst, also bin ich.“

Dieser Befund als solcher scheint bei der Mehrheit der Bürgerinnen und Bürger keine Ängste auszulösen. Aus der Horrorvision einer totalen Überwachung der Menschen ist heute weitgehend die Vorstellung geworden, durch den Einsatz von Technik und Datenerfassung würden sowohl unsere individuelle als auch unsere gesamtgesellschaftliche Sicherheit erhöht und unsere Kommunikations- und Informationsbedürfnisse besser und bequemer befriedigt. Die generelle Möglichkeit des Staates wie der Wirtschaft, sich automatisch personenbezogene Informationen zu beschaffen und diese zu verarbeiten und auszuwerten, um „Profile“ zu erstellen (Persönlichkeitsprofil, Kundenprofil, Täterprofil), erschreckt die Bürger nicht. Vor mehr als zwanzig Jahren haben viele Menschen protestiert, als sie zur Volkszählung einen Fragebogen ausfüllen sollten, dessen Daten anschließend anonymisiert wurden und die lediglich dem Staat als Planungsgrundlage dienen sollten. Die Daten, die damals erhoben wurden, waren harmlos gegenüber denjenigen, die heute angegeben werden müssen, um „Arbeitslosengeld II“ oder einen Kredit nach „Basel II“ zu beantragen, und die heute dauerhaft personenbezogen gespeichert und abgeglichen werden.

Das Bundesverfassungsgericht warnte bereits 1983: Personenbezogene Daten können – vor allem beim Aufbau integrierter Informationssysteme – zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damals kreierte das Bundesverfassungsgericht das Grundrecht auf informationelle Selbstbestimmung und formulierte den Grundsatz: „Jeder Einzelne hat die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“ Ferner

stellte es fest: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß."

Doch wer weiß heute, wer was wann und bei welcher Gelegenheit über ihn weiß? Wissen wir, was wir an persönlichen Daten wem preisgegeben haben und was mit diesen Daten geschieht? Wir müssen feststellen, dass in den 80er Jahren, als sich die Risiken einer massenhaften und schnellen automatischen Verarbeitung personenbezogener Daten gerade erst abzeichneten, der Datenschutz im Mittelpunkt des öffentlichen Interesses stand. Heute aber, da sich diese Risiken infolge technischer Machbarkeit zu realen Gefahren und Missbräuchen verdichtet haben, also der damals nur als Schlagwort beschworene „gläserne Mensch" zur Realität wird, scheint die Sensibilität für die Bedeutung des Datenschutzes als Schutz des Persönlichkeitsrechts des Bürgers und seiner Privatsphäre weitgehend abhanden gekommen zu sein.

Was sind die Gründe? Entscheidend ist wohl: Wir sehen heute – zumindest in Deutschland – keine Institution, weder auf Seiten des Staates noch der Wirtschaft, die eine totale Überwachung des Menschen vorzunehmen sich anschickt. Der Topos „Informationsgesellschaft" wird positiv empfunden. Die inzwischen alltägliche Gewöhnung an Informations- und Kommunikationstechnik, die allgegenwärtige Datenverarbeitung (ubiquitous computing) lässt Warnungen vor Missbräuchen als Ausdruck von Technikfeindlichkeit und Rückständigkeit erscheinen. Die gesellschaftliche und politische Komplexität in unserer Wissensgesellschaft ist so gestiegen, dass sich der Einzelne ohne technische Unterstützung überfordert fühlt. Ohne permanenten Datenaustausch scheint eine adäquate Teilnahme an der arbeitsteiligen Gesellschaft gar nicht mehr möglich zu sein. Wir kommen nicht umhin, uns in der Arbeitswelt und im Alltag der EDV-Technik zu bedienen und uns auf diese Technik zu verlassen.

Die Dynamik der Informations- und Kommunikationstechnik, die fortschreitende Digitalisierung und Miniaturisierung dieser Technik bei gleichzeitiger Produktverbilligung lässt uns diese Technik als Erleichterung und Verbesserung der komplexen Lebens- und Arbeitsbedingungen wahrnehmen und die zugleich eröffneten Missbrauchsmöglichkeiten verdrängen. Die politischen Herausforderungen, die Bekämpfung des internationalen Terrorismus, Konsequenzen der Globalisierung, die Umstrukturierung der Sozialsysteme, Privatisierung und Verwaltungsmodernisierung, all dies erzeugt einen enormen Handlungsdruck und Regelungsstress, angesichts dessen Datenschutz vielfach als Stör- und Kostenfaktor betrachtet wird, der sinnvolle und effektive Lösungen be- oder verhindert.

Die Notwendigkeit einer wirksamen unabhängigen Kontrolle dieser Eigendynamik staatlichen und wirtschaftlichen Handelns zur Sicherung des Persön-

lichkeitsrechts und der Privatsphäre wird oft erst dann erkannt, wenn der Einzelne ganz persönlich erlebt, dass mit seinen Daten fahrlässig oder gar missbräuchlich umgegangen wird, und er sich selbst nicht in der Lage sieht, dagegen anzugehen. Die hohe Zahl der Eingaben, die an den Hamburgischen Datenschutzbeauftragten herangetragen werden, belegt, das Datenschutz sich keineswegs von selbst durchsetzt, sondern immer wieder eingefordert und verteidigt werden muss.

Dabei werden die Begehrlichkeiten sowohl von Seiten des Staates als auch der Wirtschaft nach einer Erfassung, Sammlung und Nutzung personenbezogener Daten immer stärker. Für den Bereich der Verbrechensbekämpfung fordert die Polizei „das volle Programm". Immer weitergehende datenerhebende Instrumentarien für Vorfeldermittlungen werden eingefordert, um unabhängig von der Eingriffsschwelle des klassischen Polizeirechts, also vom Vorliegen einer konkreten Gefahr oder eines Anfangsverdachts, tätig werden zu können. Stichwort: Verdachtsunabhängige Personenkontrollen an jedem Ort in der Stadt, Videoüberwachung im öffentlichen Raum. Damit bezieht die Polizei völlig unbeteiligte und gesetzestreue Bürger in ihre Beobachtung ein. Die Polizei erhält wegen der Heimlichkeit dieser Vorfeldtätigkeit Instrumente, die bisher nur dem Verfassungsschutz zugestanden wurden. Mit dieser Art der Verdachtsschöpfung wird die Unschuldsvermutung für den Bürger unterlaufen. Der beobachtungsfreie Raum wird für den Bürger immer enger und letztlich auf den „absoluten Kernbereich privater Lebensgestaltung" reduziert. Hinzu kommt die Vorratsdatenspeicherung aller Telekommunikationsverbindungen für künftig mindestens sechs Monate. Die Polizei sagt: Neue Verbrechensformen wie Terrorismus und organisierte Kriminalität erfordern eingriffstiefere Instrumente, um den Tätern nicht bloß hinterherzulaufen. Wer hier den verfassungsrechtlich gebotenen Nachweis der Erforderlichkeit und der Verhältnismäßigkeit der Eingriffe einfordert, setzt sich dem Vorwurf des Täterschutzes aus.

Die Wirtschaft will vor dem Hintergrund sinkender Zahlungsmoral, eines weitreichenden Vollstreckungsschutzes, angesichts hoher Arbeitslosigkeit und immer unsicherer werdender Einkommensverhältnisse zur Minimierung wirtschaftlicher Risiken den Kunden durchschauen und bewerten. Mit einer möglichst großen Menge gesammelter Daten wird der Kunde deshalb in seiner Kreditwürdigkeit sowie seiner Zahlungsfähigkeit und -willigkeit kategorisiert, mit einem Score-Wert belegt. Heute fällt keine Kreditentscheidung und kaum noch eine sonstige kommerzielle Entscheidung ohne Scoring-Verfahren. Der Kunde soll ferner in seinem Verbraucherverhalten erfasst und für gezielte Werbung erschlossen werden. Um dies durchzusetzen, fordert die Wirtschaft immer mehr die Einwilligung des Kunden in eine Personalisierung als zwingende Zugangsvoraussetzung für die Teilnahme am Konsum. Dies führt zu einem Verlust der Möglichkeit der Anonymität für den Kunden, für den Bürger. Die durch immer kostengünstigere Genanalyse erzielbaren Aussagen über die geneti-

sche Disposition eines Menschen lassen die Begehrlichkeit von Versicherern, Arbeitgebern und sonstigen Interessenten steigen, diese Daten zur Risikoabschätzung zu erlangen.

Diese Entwicklungen und Tendenzen zu Lasten des Datenschutzes werden in den im Tätigkeitsbericht im Einzelnen dargestellten Sachverhalten sichtbar.

Wie stark ist das Grundrecht auf informationelle Selbstbestimmung gegenüber diesen Begehrlichkeiten? Gesetzliche Einschränkungen des Rechts auf informationelle Selbstbestimmung sind weitgehend zulässig, da die Anerkennung des Rechts auf informationelle Selbstbestimmung durch einen Gesetzesvorbehalt „erkauft“ wurde. Dieser Gesetzesvorbehalt hat nicht eingriffshemmend gewirkt. Vielmehr haben die Gesetzgeber in Bund und Ländern von der Einschränkungsmöglichkeit des Rechts auf informationelle Selbstbestimmung durch Gesetz massiv Gebrauch gemacht, wobei trotz eines hohen Detaillierungsgrades der Regelungen letztlich Abwägungsklauseln zur Anwendung kommen. Die Gesetzgeber haben dabei mehrfach den Grundsatz der Verhältnismäßigkeit verletzt und die verfassungsrechtlich einzuhaltende Grenze der Erforderlichkeit der Eingriffe überschritten und mussten von den jeweiligen Verfassungsgerichten in ihre Grenzen verwiesen werden.

Hier hat sich wiederum das Bundesverfassungsgericht als Leuchtturm für den Datenschutz und das Grundrecht auf informationelle Selbstbestimmung erwiesen, das in seinen Entscheidungen zur akustischen Wohnraumüberwachung, zur präventiven Telekommunikationsüberwachung und zur Beschlagnahme von Mobiltelefonen klare rechtsstaatliche Standards gesetzt hat.

Die wachsenden Gefährdungen der informationellen Selbstbestimmung des Einzelnen durch die Wirtschaft sind nur schwer abzuwehren, da sich das Grundrecht auf informationelle Selbstbestimmung in seiner Abwehrwirkung in erster Linie gegen den Staat richtet. Das für die Wirtschaft geltende Bundesdatenschutzgesetz erweist sich in der konkreten Anwendung oft als „Papiertiger“. Die Wirtschaft nutzt auf der Grundlage des Prinzips der Vertragsfreiheit ihre Angebotsmacht dazu aus, den Kunden über Anreizsysteme, Kundenbindungsprogramme sowie abverlangte Einwilligungserklärungen zu personalisieren und zur Preisgabe seiner persönlichen Daten zu bewegen. Stichworte: Preisausschreiben, Gewinnspiele, Bonus-Cards, LifeStyle-Umfragen. Die so erlangte Einwilligung des Kunden in die – wie es z. B. im „Kleingedruckten“ heißt – „Unterbreitung interessanter Informationen“ und „Bearbeitung seiner Daten zu Marketingzwecken“, auf die sich die Marketingstrategen und Call-Center bei ihrer Telefonwerbung berufen, erfüllt dabei wegen fehlender Bestimmtheit sehr oft nicht die gesetzlichen Anforderungen an eine informierte Einwilligung.

Welche Fragestellungen und Herausforderungen für den Datenschutz ergeben sich daraus?

Sehen wir uns – ausgelöst durch den 11.9.2001 – auch in Deutschland einer staatlichen „Überproduktion“ von Sicherheit ausgesetzt, die weit über den Bereich der Bekämpfung des Terrorismus und der organisierten Kriminalität hinausgreift? Nehmen wir wahr, dass der Bereich, in dem sich der Bürger unbeobachtet und unerfasst bewegen kann, immer enger wird, dass der Bürger auch durch gesetzestreues Verhalten einer Überwachung nicht mehr ausweichen kann? Fühlen wir uns dadurch in unserem Recht auf freie Entfaltung unserer Persönlichkeit beeinträchtigt oder empfinden wir dies als angemessenen Preis für mehr Sicherheit? Welche „Sicherheit“ ist genug? Welche Risiken müssen und wollen wir in Kauf nehmen? Ist uns bewusst, dass wir mit jedem Schritt, der zu mehr Sicherheit führen soll, zugleich etwas von unserer Freiheit und unserem Recht auf Selbstbestimmung aufgeben? Akzeptieren wir angesichts der technisch basierten Informationsgesellschaft, dass Privatheit, d.h. Unbeobachtetheit und Bewegungsfreiheit, letztlich nur noch durch Technikabstinenz erlangt werden kann? Sehen wir uns durch den Verlust von Anonymität in unserer Entscheidungsfreiheit gefährdet oder empfinden wir Personalisierung als Entscheidungshilfe und Serviceleistung? Wird uns der Verlust von Anonymität überhaupt bewusst? Registrieren wir die starke Zunahme von Datenströmen gerade auch im nicht-öffentlichen Bereich, die zu einer immer engeren Verknüpfung aller Daten führen, und erkennen wir, dass es damit möglich wird, durch Profilbildung das Verhalten eines Menschen ohne dessen Wissen und Wollen abzubilden und ihn berechenbar zu machen? Ist es erforderlich, gesetzliche Regelungen zur Beschränkung der Profilbildung und der Scoring-Verfahren sowie zur Begrenzung zentraler Auskunftssysteme zu schaffen?

Es ist zu konstatieren, dass diese Fragen im politischen Raum nicht ausreichend diskutiert werden. In einem gesellschaftlichen Klima, in dem von Politikern weitgehend unwidersprochen absoluter Vorrang für Sicherheitsfragen eingefordert werden kann, in dem Datenschutz sich dem Vorwurf ausgesetzt sieht, er dränge sich in den Vordergrund, müsse jedoch zu Gunsten vermeintlich vorrangiger Rechtsgüter zurücktreten, finden diese Fragestellungen keine besondere öffentliche Beachtung. Da bei unternehmerischen Aktivitäten der wirtschaftliche Erfolg zunehmend von der Menge der zur Verfügung stehenden personenbezogenen Daten und ihren Verknüpfungsmöglichkeiten abhängt, werden datenschutzrechtliche Forderungen nach Datenvermeidung, Datensparsamkeit und Einhaltung der Zweckbindung der Daten von der Wirtschaft als kontraproduktiv empfunden mit der Folge, dass versucht wird, diese Forderungen zu umgehen.

Um dieser Schieflage, in die der Datenschutz geraten ist, zu begegnen, müssen wir über die freiheitssichernde Funktion des Datenschutzes einen breiten gesellschaftlichen Diskurs in Gang setzen, damit das Grundrecht auf informationelle Selbstbestimmung nicht ausgehöhlt wird. Die Strukturen der Informationsgesellschaft müssen weiterhin auf eine freiheitliche, selbstbestimmte Kommunikation ausgerichtet sein, nicht auf Überwachung. Datenschutz muss

seinem Verfassungsrang entsprechend auch gegenüber neuen gesellschaftlichen Herausforderungen und neuen technischen Entwicklungen und Gefährdungen durchgesetzt werden, um zum Schutz des Persönlichkeitsrechts beizutragen und es dem Einzelnen zu ermöglichen, seine Privatsphäre zu erhalten.

Dieser Aufgabe widmen sich alle Mitarbeiterinnen und Mitarbeiter der Dienststelle engagiert und mit Nachdruck. Dafür möchte ich ihnen an dieser Stelle danken.

Der hier vorgelegte 20. Tätigkeitsbericht, der die Berichtsperiode 2004 / 2005 umfasst, ist mein erster Tätigkeitsbericht, der an den 19. Tätigkeitsbericht 2002 / 2003 anschließt, der von meinem Vorgänger Herrn Dr. Hans-Hermann Schrader vorgelegt wurde. Auch die ersten neun Monate dieses Berichtszeitraums fallen noch in die Amtszeit von Herrn Dr. Schrader. Der Amtswechsel fand am 22. September 2004 statt. Damit konnte Herr Dr. Hans-Hermann Schrader, der das Amt des Hamburgischen Datenschutzbeauftragten über 2 Amtsperioden ausgeübt hat und dessen nochmalige Wiederwahl daher nicht zulässig war, nach über 13 Jahren höchst erfolgreicher, anerkannter und nachhaltiger Arbeit für den Datenschutz und die Gewährleistung des Grundrechts auf informationelle Selbstbestimmung in den verdienten Ruhestand treten.

1. Informations- und Kommunikationstechnik

1.1 E-Government in der Metropolregion

Die erforderliche datenschutzrechtliche Bewertung des Projekts kann erst nach Vorlage der bereichsspezifischen Konzepte erfolgen.

Zur Metropolregion Hamburg gehören neben der Hansestadt 14 Kreise aus Niedersachen und aus Schleswig-Holstein. Hier leben vier Millionen Menschen. Ziel dieses Projektes ist es, einen länderübergreifenden E-Government-Service aufzubauen, der es den Verwaltungskunden ermöglicht, sich mit ihren Anliegen an jede Verwaltung in der Metropolregion wenden zu können. Als typisches Beispiel wird der Umzug genannt, bei dem eine Person von der Gemeinde A in die Gemeinde B zieht und sich dann zur Ummeldung des Wohnsitzes und des KFZ an die Verwaltung in der Gemeinde C wenden kann, weil diese für sie z. B. verkehrsgünstig auf dem Weg zur Arbeitsstelle zu erreichen ist. Diese beiden Ummeldungen wurden im Projekt exemplarisch herausgegriffen, um hierfür sach- und kundengerechte Lösungen anzubieten.

Die Landesdatenschutzbeauftragten der drei beteiligten Länder haben mit den Projektverantwortlichen Anfang 2005 erörtert, dass detaillierte Konzepte aufzustellen sind, die als Grundlage für eine datenschutzrechtliche Bewertung

dienen. In diesen Konzepten sollen neben einer differenzierten Beschreibung der Verfahrensabläufe u. a. folgende Fragen beantwortet werden:

- Welche Daten werden in den einzelnen Prozess-Schritten von den beteiligten Stellen verarbeitet?
- Auf welcher Rechtsgrundlage und in welcher rechtlichen Beziehung zueinander agieren die einzelnen Stellen?
- Wer ist Daten verarbeitende Stelle und wer trägt welche (Teil-)Verantwortung?
- Welche Prüf- und Entscheidungsaufgaben hat die jeweilige Stelle?
- Welche Abläufe und Zuständigkeiten sind bei potentiellen Konfliktfällen wie z. B. bei Widersprüchen gegen Bescheide vorgesehen?

Die Entwürfe für die bereichsspezifischen Konzepte liegen bisher noch nicht vor, so dass eine datenschutzrechtliche Bewertung noch aussteht.

1.2 HamburgGateway – das Tor zu den E-Government-Anwendungen

Digitale Zertifikate und die Nutzung des OSCI-Standards können die Sicherheit noch weiter erhöhen.

Mit dem HamburgGateway steht ein einheitlicher Zugang für die E-Government-Anwendungen der Freien und Hansestadt zur Verfügung. Zum einen werden über diesen Zugang zahlreiche Informationsangebote zur Verfügung gestellt, die ohne Registrierung abrufbar sind. Zum anderen können Bürger, Firmen oder auch Behörden diesen Dienst für Transaktions-Angebote nutzen, für die eine vorherige Registrierung erforderlich ist. In diesen Fällen prüft das Gateway, ob eine Registrierung vorliegt und ob Benutzerkennung und Passwort korrekt sind. Wenn es sich um ein kostenpflichtiges Angebot handelt, erfolgt die Bezahlung ebenfalls online über das Gateway.

Zur Zeit werden zwölf Anwendungen angeboten, davon richten sich fünf nicht nur an spezielle Verwaltungskunden wie Unternehmen und Institutionen, sondern auch an alle Bürgerinnen und Bürger. Alle Daten, die im Internet mit dem HamburgGateway ausgetauscht werden, werden SSL-verschlüsselt übertragen. Sensible personenbezogene Daten werden über die derzeitigen Anwendungen nicht verarbeitet, so dass die Prüfung von Benutzerkennung und Passwort einen ausreichenden Schutz gegen eine missbräuchliche Nutzung bietet.

Das HamburgGateway könnte zusätzlich auch dazu genutzt werden, elektronische Post zwischen Bürgern und Behörden auszutauschen. Die elektronischen Mitteilungen wären durch die Verschlüsselung insbesondere vor einer unberechtigten Kenntnisnahme im Internet geschützt. Es wäre der Vorteil einer solchen Lösung, dass die Bürger für die Verschlüsselung keine zusätzliche Software installieren müssten. Da im HamburgGateway bereits einzelne

Module für eine virtuelle Poststelle vorhanden sind, werden wird uns dafür einsetzen, dass dieser Dienst kurzfristig angeboten wird.

Der „4. Hamburger E-Government Aktionsfahrplan“ sieht mittelfristig eine Ausweitung der Anzahl der angebotenen Verfahren vor. Darunter befinden sich dann auch Anwendungen, bei denen sensiblen personenbezogenen Daten ausgetauscht werden sollen. Für solche Verfahren sind zur Sicherstellung des Datenschutzes ergänzende technische Maßnahmen erforderlich. Im Aktionsfahrplan ist ausgeführt, dass dafür das Produkt Governikus zügig implementiert werden kann, das auf dem OSCI-Standard (Online Services Computer Interface) aufsetzt. Dieser Standard, der für E-Government-Anwendungen des Bundes vorgeschrieben ist, bietet nicht nur den Vorteil einer sicheren Authentisierung auf der Grundlage digitaler Zertifikate, sondern auch eine erhöhte Sicherheit zum Schutz der Vertraulichkeit, da die Inhaltsdaten auf der gesamten Übertragungsstrecke zwischen dem Nutzer und der Daten verarbeitenden Stelle in der Verwaltung verschlüsselt sind.

Mit OSCI steht bereits ein bewährter Sicherheits-Standard für E-Government-Anwendungen zur Verfügung. Verfahren, die diese Standards berücksichtigen, bieten die Gewähr für eine durchgehende Sicherheit bei der Datenübermittlung vom Versand bis zum Empfang (Ende-zu-Ende-Sicherheit) und erlauben somit auch rechtsverbindliche Transaktionen zwischen den beteiligten Kommunikationspartnern.

Die durchgehende Sicherheit darf nicht dauerhaft durch Vermittlungs- und Übersetzungsdienste, die nicht der OSCI-Spezifikation entsprechen, beeinträchtigt werden. Werden solche Dienste zusätzlich in die behördlichen Kommunikationsströme eingeschaltet, wird das mit OSCI-Transport erreichbare Sicherheitsniveau abgesenkt. Der Einsatz von sogenannten Clearingstellen, wie sie zunächst für das automatisierte Meldeverfahren vorgesehen sind, kann daher nur eine Übergangslösung sein.

Werden Programme und Schnittstellen auf Standards wie OSCI entwickelt, ist sichergestellt, dass die Produkte verschiedener Anbieter im Wettbewerb grundlegende Anforderungen des Datenschutzes und der Datensicherheit in vergleichbar hoher Qualität erfüllen. Gleichzeitig erleichtern definierte Standards den öffentlichen Verwaltungen die Auswahl datenschutzkonformer, interoperabler Produkte.

Vor diesem Hintergrund hat die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die vom Koordinierungsausschuss Automatisierte Datenverarbeitung (KoopA ADV), dem gemeinsamen Gremium von Bund, Ländern und Kommunalen Spitzenverbänden, getroffene Festlegung begrüßt, in E-Government-Projekten den Standard OSCI-Transport für die Übermittlung von personenbezogenen Daten einzusetzen. Um die angestrebte Ende-zu-

Ende-Sicherheit überall zu erreichen, empfiehlt die Konferenz einen flächendeckenden Aufbau einer OSCI-basierten Infrastruktur.

1.3 Verwendung privater PDA nur nach Genehmigung

Privat beschaffte Software auf PDA muss vor einem Anschluss an das FHH-Netz freigegeben werden.

Mit Personal Digital Assistents (PDA) stehen mobile Computer mit großem internen Speicher, vielfältigsten Anwendungsprogrammen und häufig mit einer drahtlose Kommunikationsschnittstelle zur Verfügung. Kritisch ist zu sehen, dass keine Trennung zwischen Nutzung und Administration des Geräts vorliegt. Programme zum Schutz der Geräte gegen Angriff und Missbrauch liegen noch immer nicht mit gleich hoher Qualität vor wie z. B. für Laptops. Selbst wenn der PDA nur als elektronischer Terminkalender genutzt wird, kann das Schadenspotential eines solchen Gerätes durch bewusste, irrtümliche oder nachlässige Fehlnutzung beträchtlich sein. Pressemitteilungen über Viren auf PDA zeigen, wie real diese Bedrohung ist.

Der Einsatz von PDA in der hamburgischen Verwaltung wurde von der Finanzbehörde mit der am 1.6.2005 erfolgten Neufassung der PC-Richtlinie geregelt. Auch wenn sich der Hamburgische Datenschutzbeauftragte mit seiner Position nicht durchsetzen konnte, den Anschluss privater Geräte und damit auch privater PDA an dienstliche PC wegen des vorhandenen Gefährdungspotentials generell zu untersagen, konnte zumindest erreicht werden, dass für den Einsatz von PDA strenge Regeln erlassen wurden. Dazu gehört:

- Der für die IuK-Technik Verantwortliche ist vorab über den Betrieb und Anschluss privat beschaffter PDA zu informieren und hat den Betrieb zu genehmigen.
- Die Nutzer mobiler Geräte sind durch die zuständige Geräteadministration in die vorschriftsmäßige Handhabung eines Notebooks bzw. PDA einzuweisen und über die geltenden Sicherheitsvorschriften zu informieren.
- Werden sensible Daten, insbesondere sensible personenbezogene Daten oder besonders schutzwürdige Sachdaten gespeichert, sind diese auf den Speichermedien durch eine geeignete Verschlüsselungssoftware zu schützen.
- Der Betrieb und Festnetzanschluss dienstlich sowie privat beschaffter PDA an Geräte des FHH-Netzes ist nur zulässig, wenn zur Synchronisation die in der geltenden IuK-Architektur-Richtlinie zugelassene Software benutzt wird.
- Während der Leitungsanbindung an das FHH-Netz sind drahtlose Verbindungen technisch zu unterbinden.

- Wird ein PDA an ein Netzwerk oder zur Synchronisation an Endgeräte angeschlossen, muss zunächst soweit möglich auf dem mobilen Endgerät eine Aktualisierung des Virenscanners erfolgen bzw. ein aktueller Virenscanner aufgespielt werden, ferner müssen alle zu synchronisierenden Dateien vor einer weiteren Verarbeitung auf Viren gescannt werden.
- Darüber hinaus muss die auf einem PDA eingesetzte nicht dienstlich beschaffte Software ebenfalls durch die zuständige IuK-Stelle geprüft und freigegeben werden.

Durch diese Regelungen wird das Risiko der PDA-Nutzung reduziert. Die Behörden sind aufgefordert, diese Regelung unverzüglich umzusetzen, zumal die Finanzbehörde explizit darauf hingewiesen hat, dass auch bereits im Einsatz befindliche PDA entsprechend dieser Richtlinie zu behandeln sind.

1.4 Test mit Originaldaten in der Freigabe-Richtlinie neu geregelt

Eine Freigabe von IT-Verfahren erfordert immer systematisch entwickelte Testdaten.

Behörden, die neue IT-Verfahren anwenden wollen, tragen immer wieder den Wunsch an uns heran, einen Test mit Originaldaten zuzulassen. Aus Prüfungen und Gesprächen wissen wir, dass in vielen Fällen solche Tests sogar stattfinden, ohne dass die Datenschutzaspekte eingehend problematisiert wurden. Dabei sind die Motive vielfältig: Sei es aus Zeitdruck im Projekt, der dazu führt, dass die Bildung von Testdaten zu aufwändig erscheint, sei es, weil Massentests schnell durchgeführt werden sollen oder weil die Auffassung besteht, mit Originaldaten alle Testerforderlichkeiten erfüllt zu haben.

Bei der Nutzung von Originaldaten zu Testzwecken kann es zu gravierenden Verletzungen schutzwürdiger Interessen der Betroffenen kommen, da häufig die technischen und organisatorischen Sicherheitsmaßnahmen im Testbereich nicht denen der Produktionsumgebung entsprechen, der Personenkreis, der die Daten zur Kenntnis nehmen kann, erweitert wird und Daten im Rahmen der Tests verfälscht werden können. Es ist ferner zu beachten, dass die Verarbeitung der Originaldaten der Zweckbindung unterliegt. Der Test mit Originaldaten wird von diesem Zweck in der Regel nicht erfasst.

In intensiven Gesprächen mit den beteiligten Stellen konnten wir verhindern, dass Originaldaten ständig und ohne Vorbedingungen für Testläufe genutzt werden. Mit der Fortschreibung der Freigabe-Richtlinie durch die Finanzbehörde wurde ein Kompromiss zwischen den Anforderungen des Datenschutzes und den Anforderungen der IT-Entwickler nach praktikablen Lösungen gefunden.

Für alle IT-Verhaben sind in der neuen Freigaberichtlinie Funktions- und Abnahmetests vorgeschrieben. Diese Tests basieren auf drei Grundprinzipien:

- „Software und DV-Verfahren sind mit systematisch entwickelten Fall-Konstellationen (Testdaten) nach einem Testplan, aus dem das gewünschte Ergebnis hervorgeht, zu überprüfen.
- Ergänzende Massendatentests können – wenn erforderlich – nach Zustimmung und Vorgabe der Fachlichen Leitstelle mit anonymisierten Originaldaten durchgeführt werden. (...)
- Zu Testzwecken darf eine Kopie der erforderlichen Originaldatensätze verwendet werden, wenn eine andere Rechtsvorschrift dies ausdrücklich erlaubt oder falls sich im Ausnahmefall trotz Nachbildung im Testbereich ein Fehler aus dem Produktionsbetrieb nicht ermitteln, sondern nur mit Originaldaten aufklären lässt, oder die Verfahrenssicherheit nicht anders gewährleistet werden kann, wenn
  - eine bereichsspezifische Rechtsvorschrift dies nicht ausdrücklich untersagt,
  - eine Anonymisierung der Originaldaten für die vorgesehene Test-Konstellation nur mit einem unvertretbar hohem Aufwand verbunden wäre,
  - die Fachliche Leitstelle dem Vorgehen schriftlich zugestimmt hat,
  - bei der Durchführung oder Auswertung des Tests die schutzwürdigen Belange der Betroffenen und die Datensicherheit angemessen berücksichtigt werden,
  - sichergestellt ist, dass nur die für die Fehlerbehebung und Durchführung des Tests erforderlichen Personen die Daten nutzen können und
  - Zugang zu diesen Daten nur Personen erhalten, die den jeweils maßgebenden Vertraulichkeitsgrundsätzen und insbesondere datenschutzrechtlichen Vorschriften unterliegen.“

Da das erste Grundprinzip keine Ausnahmen vorsieht, sind für alle DV Verfahren systematische Testdaten zu entwickeln, wobei der Umfang und die Komplexität der Testfälle aufgrund der jeweiligen Bedingungen festzulegen sind. Auch wenn im Einzelfall Tests mit Originaldaten zulässig sind, reicht es somit nicht, die Tests ausschließlich mit diesen Originaldaten durchzuführen.

Die Einhaltung dieser Richtlinie werden wir bei Prüfungen und der Einführung neuer IT-Verfahren verstärkt überprüfen.

1.5 Dokumentenverwaltung ELDORADO

Die datenschutzrechtliche Verantwortung für die Verarbeitung personenbezogener Daten beim Einsatz der elektronischen Dokumentenverwaltung ELDORADO liegt bei den für die Datenverarbeitung verantwortlichen Stellen in den Behörden und Ämtern.

Im 18. Tätigkeitsbericht (18.TB, 3.4) hatten wir bereits verschiedene Problemfelder in Bezug auf die bisher in Papierakten und künftig in elektronischen Akten enthaltenen personenbezogenen Daten aufgezeigt. Um die Erfüllung der datenschutzrechtlichen Anforderungen bei der Einrichtung und Ausgestaltung des Verfahrens und auch im täglichen Umgang mit der Automation zu gewährleisten, haben wir auf die Erforderlichkeit der Erstellung verbindlicher, einheitlicher Vorgaben für die Behörden und Ämtern hingewiesen (19.TB, 3.3).

Im Dezember 2004 wurde zwischen der Freien und Hansestadt Hamburg und den Spitzenorganisationen der Gewerkschaften eine Vereinbarung nach § 94 des Hamburgischen Personalvertretungsgesetzes (HmbPersVG) über den Einsatz von ELDORADO geschlossen. Zudem wurde unter unserer Mitwirkung eine IT-Richtlinie zum Umgang mit ELDORADO erstellt, welche im Januar 2005 in das IT-Handbuch der Stadt aufgenommen wurde. Diese gilt jedoch nicht für die Verarbeitung personenbezogener Daten, die durch spezialgesetzliche Regelungen besonders geschützt sind.

Eine im Dezember 2005 von der Finanzbehörde vorgelegte Risikoanalyse für das bei Dataport betriebene Verfahren ELDORADO befindet sich zurzeit in der Abstimmung. Betrachtet wird hierin ausschließlich die vorgesehene Verarbeitung personenbezogener Inhaltsdaten der Schutzbedarfskategorie „niedrig bis mittel“ (nach der 3-stufigen Skala des BSI). Die Risikoanalyse gilt ausdrücklich nicht für Verfahren, in denen personenbezogene Daten / Inhalte der Schutzkategorie „hoch“ oder „sehr hoch“ verarbeitet werden. Ebenso sind Einzelfallakten, die sich auf Beschäftigte beziehen und / oder Akten, für die besondere datenschutzrechtliche Anforderungen gelten, davon ausgeschlossen. Gleiches gilt, wenn teraDOC lediglich als Archivkomponente eingesetzt wird. Entsprechende Verfahren sind gesondert zu betrachten.

Die zentrale technische Bereitstellung des Dokumentenverwaltungssystems entbindet die für die Datenverarbeitung verantwortlichen Stellen (§ 4 Abs. 3 HmbDSG) nicht von ihrer datenschutzrechtlichen Verantwortung. Vor der Entscheidung über die Einführung des Verfahrens und die Aufnahme von Akten in die ELDORADO-Aktenverwaltung ist auch eine Analyse der in den Akten enthaltenen personenbezogenen Daten erforderlich. Erst anhand einer entsprechenden Schutzbedarfsbewertung der vorhandenen Aktenkategorien durch die verantwortlichen Stellen kann die notwendige Prüfung erfolgen, ob mit den

verfügbaren Schutzmechanismen ein angemessenes Schutzniveau erreicht werden kann.

1.6 Verschlüsselter E-Mail-Verkehr in der hamburgischen Verwaltung

Zur Verschlüsselung von E-Mails mit sensiblen Daten steht für die Behörden das Instrument der „Erweiterten Sicherheit" zur Verfügung. Die Bereitstellung und Anwendung dieses Instruments verläuft in den Behörden und Ämtern leider sehr schleppend.

Die „Erweiterte Sicherheit" ist eine in Outlook bereitgestellte Funktionalität zur Verschlüsselung von E-Mails, die innerhalb des Bereichs des FHHinfoNET verschickt werden. Die Verschlüsselung von sensiblen personenbezogenen Daten ist nicht nur eine Forderung des Hamburgischen Datenschutzbeauftragten, sondern eine vom Senat festgelegte verbindliche Verpflichtung auf der Grundlage der § 94er-Vereinbarung „Bürokommunikation". So hat der Senat mit der Drucksache 18 / 929 vom 21.9.2004 unter der Textziffer 3.6 gegenüber der Bürgerschaft ausgeführt:

> „Insbesondere stimmt der Senat dem Hamburgischen Datenschutzbeauftragten zu, dass sensible Personal-, Gesundheits- und Sozialdaten vorrangig zu verschlüsseln sind. Dementsprechend bestimmt Nummer 6 der Allgemeinen Regeln für die Bürokommunikation, dass besonders sensible, insbesondere sensible personenbezogene Daten, elektronisch nur verschlüsselt übermittelt werden dürfen."

Neben der eindeutigen Beschlusslage steht mit der „Erweiterten Sicherheit" auch praktisch ein Instrument zur Verfügung, das von allen Behörden und Ämtern genutzt werden kann. Der geringe Einführungsaufwand bei aktuellen Betriebssystemen und Softwareständen steht einem zügigen Roll-Out nicht entgegen. Dennoch verläuft die flächendeckende Einführung bei den betroffenen Arbeitsplätzen sehr schleppend. Es gibt zwar einzelne Behörden, die alle einschlägigen Arbeitsplätze mit der Erweiterten Sicherheit ausgestattet haben oder dieses kurzfristig im Rahmen der ESARI-Einführung realisieren werden, aber bei vielen Behörden steht die Verschlüsselung des Mail-Verkehrs noch nicht auf der Agenda. Da aufgrund der Rechtslage sensible personenbezogene Daten ohne Verschlüsselung auch nicht innerhalb des hamburgischen Verwaltungsnetzes per E-Mail verschickt werden dürfen, wird dadurch der kundenorientierte und effiziente Bearbeitungsprozess immer wieder behindert.

Werden sensible personenbezogene Daten unverschlüsselt per E-Mail übermittelt, kommt es zu einem Verstoß gegen datenschutzrechtliche Anforderun-

gen, wie z. B. beim Berichtswesen der Staatsanwaltschaft an die Justizbehörde. Solange hier keine Verschlüsselung erfolgt, müssen die Berichte mit der Behördenpost im verschlossenen Umschlag übersandt werden. Gegenüber der Justizbehörde haben wird daher die Forderung aufgestellt, in Berichtssachen bei der Staatsanwaltschaft und der Justizbehörde die „Erweiterte Sicherheit“ umgehend einzuführen und zu nutzen. Die Umsetzung dieser Forderung werden wir mit Nachdruck verfolgen.

Der Hamburgische Datenschutzbeauftragte hat sich auch in diesem Berichtszeitraum in zahlreichen Gesprächen mit den Verantwortlichen aus den Behörden und Ämtern dafür eingesetzt, die Realisierung der Erweiterten Sicherheit zu beschleunigen und nun endlich den Beschäftigten den Zugang zur Nutzung der Erweiterten Sicherheit zu ermöglichen. Die Reaktion der Verantwortlichen ist aus der Sicht des Hamburgischen Datenschutzbeauftragten jedoch nach wie vor unbefriedigend.

1.7 Risiken durch RFID-Chips

Beim Einsatz von RFID-Chips werden häufig personenbezogene Daten verarbeitet. Daher sind spezifische Sicherheitsmaßnahmen erforderlich. Der Einsatz von RFID-Chips muss für die Nutzer transparent gestaltet sein.

Die Radio Frequency Identification (RFID) – Technologie kann als automatisches Identifikations- und Datenerfassungssystem mit kontaktloser Datenübermittlung auf Basis der Radiofrequenztechnologie definiert werden. Diese Technologie wird bisher hauptsächlich in den Bereichen Industrieautomation, Zutrittssysteme, Tieridentifikation, Warenmanagement und bei elektronischen Wegfahrsperren angewendet. Die RFID-Chips sind häufig so klein, dass nicht zu erkennen ist, dass ein Gegenstand einen RFID-Chip enthält. Die besondere Brisanz dieser Technologie liegt in der Möglichkeit, die auf dem Chip gespeicherten Daten über eine Entfernung von bis zu einigen Metern funkgesteuert auslesen und ggf. verändern zu können. Da keine Mitwirkung des Besitzers des mit einem RFID-Chip versehenen Gegenstandes am Auslesevorgang erforderlich ist, kann das Auslesen auch ohne Wissen und Wollen des Besitzers erfolgen.

Jeder RFID-Chip besitzt eine weltweit eindeutige Nummer. Darüber hinaus können auf dem Chip je nach Typ umfangreiche Daten gespeichert werden. Die Rechte der Betroffenen werden häufig durch die Nutzung der RFID-Technologie tangiert. Anhand von Beispielen soll dies kurz verdeutlicht werden:

- Auf Medikamenten-Verpackungen kann im Chip eine Nummer angegeben werden, aus der sich die Bezeichnung des Medikaments eindeutig ableiten

lässt. Wenn keine zusätzlichen Schutzmaßnahmen getroffen werden, kann diese Information von Lesegeräten ausgelesen werden, in deren Reichweite die Person mit der Medikamenten-Verpackung kommt. Aus dieser Medikamenten-Nummer können Rückschlüsse auf den Gesundheitszustand gezogen werden. Weitere sprechende Nummer sind z. B. die ISBN bei Büchern oder der Electronic Product Code (EPC), eine international standardisierte Produktkennzeichnung.

- Da der RFID-Chip eine eindeutige Nummer trägt, kann diese Kennzeichnung genutzt werden, um zu dieser Nummer weitere Daten zu speichern. Eine solche Nutzung ist z. B. mit Gegenständen möglich, die eine Person häufig bei sich trägt, z. B. eine Armbanduhr oder ein Mitgliedsausweis. Auf diese Weise können Bewegungs- bzw. Anwesenheits-Profile erstellt werden, die ggf. zu einem späteren Zeitpunkt um den Namen und weitere Daten über die Person ergänzt werden können.

- Wenn auf einer RFID-Pre-Paid-Karte auch der aktuell vorhandene Geldbetrag gespeichert ist, besteht die Gefahr einer „gläsernen Geldbörse“, da auch von nicht autorisierten Personen dieser Betrag mit einem Schreib-Lesegerät ausgelesen und ggf. sogar verändert werden kann.

- Wenn eine Mitarbeiterkarte mit RFID-Chip z. B. für eine Zugangssicherung zu Räumen oder Geräten vorgeschrieben wird, kann diese Karte auch unbemerkt zur Leistungs- und Verhaltenskontrolle missbraucht werden.

In den genannten Beispielen werden personenbeziehbare Daten verarbeitet, daher müssen in diesen Fällen die Vorschriften der Datenschutzgesetze beachtet werden. Dazu gehört auch immer die Prüfung, ob die Ziele nicht auch mit einer anderen Technologie erreicht werden können, die ein geringeres Gefährdungspotential beinhaltet.

Sofern RFID-Chips verwendet werden sollen, muss vorab geklärt werden, auf welcher Rechtsgrundlage dies geschieht. In weiten Bereichen wird dafür nur die Einwilligung in Frage kommen. In Bereichen, in denen nicht von einer Freiwilligkeit ausgegangen werden kann, wie z. B. bei einer Mitarbeiterkarte im Arbeitsverhältnis, bedarf es einer Rechtsvorschrift. In jedem Fall müssen die betroffenen Nutzer umfassend über die eingesetzte Technik informiert und die spezifischen Risiken offengelegt werden. Es müssen auch technische und organisatorische Maßnahmen getroffen werden, um die Risiken möglichst weitgehend zu verringern. Die Tabelle, die das Bundesamt für Sicherheit in der Informationstechnologie (BSI) veröffentlicht hat, kann dafür herangezogen werden.

Angriff	Kosten	Gegenmaßnahmen	Kosten
Abhören der Kommunikation zwischen Tag und Lesegerät	hoch	Verlagerung ins Backend Abschirmung Verschlüsselung	mittel
Unautorisiertes Auslesen der Daten	mittel bis hoch	Detektoren Authentifizierung	mittel
Unautorisiertes Verändern der Daten	mittel bis hoch	Read-only-Tags Detektoren Authentifizierung	gering bis mittel
Cloning und Emulation	mittel	Erkennung von Duplikaten Authentifizierung	mittel
Ablösen des Tags vom Trägerobjekt	gering	Mechanische Verbindung Alarmfunktion (aktive Tags) Zusatzmerkmale	gering bis mittel
Mechanische oder chemische Zerstörung	gering	Mechanische Verbindung	gering bis mittel
Zerstörung durch Feldeinwirkung	mittel	selbst heilende Sicherung (nur begrenzt wirksam)	in Serie gering
Zerstörung durch Missbrauch eines Kill-Befehls	mittel	Authentifizierung	mittel
Entladen der Batterie (nur aktive Tags)	mittel	Schlafmodus	in Serie gering
Blocker-Tag	gering	Verbot in AGB (nur begrenzt wirksam)	gering
Störsender	mittel bis hoch	Messungen Frequenzsprungverfahren	mittel bis hoch
Feldauslöschung	gering (jedoch schwierig)	keine	-
Feldverstimmung	sehr gering	aktive Frequenznach-führung	mittel bis hoch
Abschirmung	sehr gering	verbesserte Lesestationen (nur begrenzt wirksam)	mittel

Tabelle 7-2: Angriffe auf RFID-Systeme und Gegenmaßnahmen

Sehr häufig sind RFID-Chips darüber hinaus als mobile Verarbeitungsmedien anzusehen. Dies ist immer dann der Fall, wenn nicht nur eine Datenspeicherung erfolgt, sondern auf der Karte auch Verarbeitungsprozesse stattfinden. Dazu gehören z. B. Authentisierungs- und kryptografische Prozesse.

Die Datenschutzbeauftragten der Länder und des Bundes erarbeiten derzeit eine Orientierungshilfe zur RFID-Technik, die in Kürze veröffentlicht wird.

1.8 Voice over IP (VoIP)

Das Telefonieren über das Internet erlebt zurzeit einen Boom. Triebfedern sind Kostenreduzierung und die Integration von Datenverarbeitung und Telefonie. Wesentliche Datensicherheitsprobleme sind jedoch ungelöst.

Die Leistungsfähigkeit von Computernetzwerken nimmt rasant zu. Sowohl in Firmen und Behörden wie auch im häuslichen Umfeld stehen durch Entwicklungen wie Gigabit-Ethernet, DSL und Flatrate Leitungskapazitäten in großem Ausmaß zur Verfügung. Parallel dazu existiert die davon unabhängige, vergleichsweise schmalbandige Infrastruktur der klassischen Kommunikationsform Telefon.

In Anbetracht der hohen Kosten einer solchen doppelten Infrastruktur wurden bereits vor längerer Zeit Versuche unternommen, das Internet als Trägermedium für Telefongespräche und den PC als Telefon zu nutzen. Zwar ist die Digitalisierung im Bereich der Telefonie selbst weit vorangeschritten (ISDN, digitale Vermittlung), dennoch bestehen zwischen Telefon- und Computernetzen nach wie vor wesentliche Unterschiede. Eine Telefonverbindung ist – zumindest in Hinblick auf den damit eröffneten Sprachkanal – exklusiv zwischen den Endteilnehmern. Die übertragenen Signale werden nicht von anderen Verbindungen gestört oder beeinträchtigt. Demgegenüber sind Computernetze auf Basis des TCP / IP-Protokolls viel stärker auf eine gleichzeitige Nutzung hin ausgerichtet. Ein PC kann z. B. zeitgleich mit einem Dateiserver, einem Netzwerkdrucker und mit einem Web-Server im Internet verbunden sein. Keine dieser Verbindungen wird bevorzugt behandelt. Sie nehmen aufgrund von Kapazitätsgrenzen aufeinander Einfluss, wobei Fehlerkorrekturmechanismen eine insgesamt zuverlässige Übertragung sicherstellen, solange die Kapazitätsgrenzen nicht wesentlich und nicht dauerhaft überschritten werden.

Dies hat Auswirkungen sowohl auf technische wie auf juristische Aspekte der Internettelefonie. Die Echtzeitübertragung von Sprachdaten über Computernetze kann nur dann in einer für den Nutzer befriedigenden Qualität erfolgen, wenn Verzögerungen und Ausfälle unterhalb eines bestimmten Niveaus liegen. Die Sprachdaten müssen daher mit höherer Priorität befördert, andere Daten ggf. zurückgehalten werden.

Werden Sprachdienste in Computernetze integriert, dehnen sich damit die dort bekannten Risiken (Viren, Würmer, Trojanische Pferde, Kenntnisnahme von Verbindungs- und Inhaltsdaten) auch auf den Bereich der Telefonie aus. Welche Folgen dies langfristig haben wird, lässt sich kaum vorhersehen. Feststellen lässt sich jedenfalls, dass Sicherheitsanforderungen bislang keine bestimmende Rolle bei der Entwicklung der VoIP-Technologien spielen und lediglich als zusätzliche, optionale Elemente behandelt werden.

Ob bzw. inwieweit Internet-Telefonie in den bestehenden Rechtsrahmen des Telekommunikationsgesetzes (TKG) passt, ist eine heftig diskutierte Frage. Die Bundesnetzagentur (Nachfolgerin der Regulierungsbehörde für Post und Telekommunikation, RegTP) geht in einem Eckpunktepapier davon aus, dass zumindest bestimmte VoIP-Angebote einen Telekommunikationsdienst im Sinne TKG darstellen. Aus Sicht des Datenschutzes kann es in Hinblick auf die

Wahrung des Fernmeldegeheimnisses jedenfalls nicht darauf ankommen, auf welchem technischen Wege eine Verbindung zustande kommt.

Risiken ergeben sich auch für die Sicherheit der an das gemeinsame Netz angeschlossenen Computer. Die Datennetze müssen für weitere Anwendungsbereiche eingerichtet und Firewalls entsprechend geöffnet werden. Neue Arten von Denial-of-Service-Angriffen sind denkbar.

Aus diesen Gründen hat die 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2005 eine Entschließung gefasst, die auf die Probleme dieser Technologie aufmerksam macht und erhöhte Anstrengungen einfordert, die Sicherheit beim Telefonieren über das Internet zu gewährleisten.

Wortlaut der Entschließung (Auszug)

„Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert Hersteller, Anbieter sowie Anwender von VoIP-Lösungen auf, das grundgesetzlich geschützte Fernmeldegeheimnis auch bei VoIP zu wahren und hierfür

- angemessene technische und organisatorische Maßnahmen zu treffen, um eine sichere und datenschutzgerechte Nutzung von VoIP in einem Netzwerk zu ermöglichen,
- Verschlüsselungsverfahren für VoIP anzubieten bzw. angebotene Verschlüsselungsmöglichkeiten zu nutzen,
- Sicherheits- und Datenschutzmängel, die die verwendeten Protokolle oder die genutzte Software bisher mit sich bringen, durch Mitarbeit an der Entwicklung möglichst schnell zu beseitigen,
- auf die Verwendung von offenen, standardisierten Lösungen zu achten beziehungsweise die verwendeten Protokolle und Algorithmen offenzulegen,
- VoIP-Kunden über die Gefahren und Einschränkungen gegenüber dem klassischen, leitungsvermittelten Telefondienst zu informieren und
- bei VoIP alle datenschutzrechtlichen Vorschriften genauso wie bei der klassischen Telefonie zu beachten.

In den benutzten Netzen, auf den beteiligten Servern und an den eingesetzten Endgeräten müssen angemessene Sicherheitsmaßnahmen umgesetzt werden, um die Verfügbarkeit, die Vertraulichkeit, die Integrität und die Authentizität der übertragenen Daten zu gewährleisten.“

1.9 Web-Monitoring und Usertracking

Die Analyse der Nutzung von Internet-Angeboten darf nur im Rahmen der dafür gezogenen rechtlichen Grenzen erfolgen. Dies gilt insbesondere, wenn diese Auswertungen durch Dritte erfolgen.

Viele Anbieter von Internet-Angeboten haben ein großes Interesse, die konkrete Nutzung ihrer Inhalte zu ermitteln. Ob eine bestimmte Marketingaktion tatsächlich zu einem erhöhten Surf- und. Kaufvolumen führt oder ob der Relaunch eines Angebots von den Nutzern honoriert wird, sind typische Fragen, die beantwortet werden sollen. Dabei geht es in aller Regel nicht um das individuelle Verhalten eines einzelnen Nutzers, sondern um statistisch relevante Aussagen. Allerdings werden diese über die Beobachtung des Nutzungsverhaltens jeweils individuell unterscheidbarer Nutzer gewonnen.

Da jeder einzelne Abruf bei dem im WWW (World Wide Web) verwendeten Hypertext Transfer Protocol (HTTP) unabhängig von den vorherigen erfolgt, ist die Zuordnung der verschiedener Abrufe eines Nutzers nicht ohne Weiteres verlässlich möglich. Es kommen daher Techniken zum Einsatz, die den Nutzer, der eine Web-Seite abruft, anhand bestimmter Merkmale identifizieren. Diese können entweder explizit durch den Anbieter gesetzt werden, z. B. durch Verwendung von Cookies oder Session-IDs in der Webadresse (URL, Uniform Ressource Locator). Alternativ können die automatisch übermittelten detailreichen Nutzungsinformationen (IP-Adresse, Name und Version von Browser und Betriebssystem etc.) zu einem Identifikator verdichtet werden.

Aus rechtlicher Sicht handelt es sich bei einem solchen Verfahren um die Erstellung von Nutzungsprofilen. Auch wenn es im Ergebnis nicht um die Auswertung des einzelnen Profils geht, führt das Web-Monitoring notwendigerweise über diesen personenbezogenen Zwischenschritt. Nutzungsprofile dürfen nach § 6 TDDSG (Teledienstedatenschutzgesetz) bzw. § 19 MDStV (Mediendienstestaatsvertrag) für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung des Angebots unter zwei Bedingungen erstellt werden: Die Profile müssen pseudonym sein, und der Nutzer darf ihnen nicht widersprochen haben.

Die Pseudonymität der Profile ist dann gegeben, wenn auf direkt identifizierende Merkmale wie Nutzerkennung, IP-Adresse etc. aus dem verwendeten Identifikator nicht geschlossen werden kann. Die Verwendung pseudonymer Profile steht nicht im Widerspruch zu dem beim Web-Monitoring verfolgten Ziel, so dass sich in dieser Hinsicht keine unauflösbaren Konflikte ergeben.

Schwieriger gestaltet sich die Umsetzung der Widerspruchsmöglichkeit. Das Gesetz fordert eine entsprechende Aufklärung des Nutzers durch den Anbieter. Damit diese ihren Zweck erfüllt, muss sie rechtzeitig (d.h. vor Bildung des Nutzungsprofils) und detailliert erfolgen, so dass der Nutzer seine Entscheidung für oder gegen einen Widerspruch begründet vornehmen kann. Dem Nutzer

muss zudem die Möglichkeit aufgezeigt werden, wie er der Erstellung von Nutzungsprofilen konkret widersprechen kann. Der Hinweis auf den möglichen Verzicht der Nutzung genügt hierbei ebensowenig wie der Verweis auf die Tatsache, dass durch Browsereinstellungen das Setzen von Cookies verhindert werden kann. Beides ist in diesem Zusammenhang dem Nutzer nicht zuzumuten.

Eine rechtskonforme Umsetzung wäre durch die Verwendung eines speziellen Widerspruchs-Cookies oder eines Parameters in der URL möglich, der gesetzt wird, sobald der Nutzer widerspricht (z. B. durch Klick auf einen Button oder die Nutzung eines besonderen Links). Die Cookielösung hat dabei aus Sicht des Nutzers den Vorteil, dass der Widerspruch nicht bei jeder neuen Nutzung erneut erklärt werden muss, sondern solange gilt bis er ggf. zurückgenommen wird. Erfolgt die Profilbildung bereits ab Nutzungsbeginn – was häufig der Fall ist -, muss ein (notwendigerweise) nachfolgender Widerspruch auch rückwirkend beachtet, d.h. das bis dahin erstellte Profil gelöscht werden.

Verschiedene Firmen haben sich darauf spezialisiert, das Web-Monitoring als Dienstleistung im Auftrag durchzuführen. Für den Betreiber eines Web-Angebots hat eine solche Lösung den Vorteil, dass er diese nicht zu seinem Kerngeschäft zählende Tätigkeit nicht selbst durchführen muss. In technischer Hinsicht müssen bei einer solchen Konstellation zusätzliche Nutzungsdaten für den Dienstleister erzeugt oder vorhandene an diesen übermittelt werden. Rechtlich handelt es sich um eine Datenverarbeitung im Auftrag (§ 11 BDSG), für die inhaltlich der Betreiber des Web-Angebots verantwortlich ist. Er muss sich daher davon vergewissern, dass die Erhebung und Verarbeitung der Daten durch den Dienstleister in rechtlich zulässiger Weise erfolgt. Für den Dienstleister selbst hat dies im Umkehrschluss zur Folge, dass die Verwendung datenschutzgerechter Technologien und Praktiken für den Markterfolg wesentlich ist.

Wir haben einen solchen Dienstleister in unserem Zuständigkeitsbereich geprüft und planen nach Abschluss dieser Prüfung eine Ausdehnung der Kontrollen auf andere entsprechende Firmen.

DATENSCHUTZ IM ÖFFENTLICHEN BEREICH

2. Behördliche Datenschutzbeauftragte

Erst wenige Behörden haben von der 2001 geschaffenen Möglichkeit Gebrauch gemacht, einen behördlichen Datenschutzbeauftragten zu bestellen. Wir ermutigen die Behörden, eigene Datenschutzbeauftragte zu bestellen und unterstützen diese bei der Wahrnehmung ihres Amtes.

Die Vorschrift zur Bestellung behördlicher Datenschutzbeauftragter ist im Hamburgischen Datenschutzgesetz lediglich eine Kann-Bestimmung (§ 10a HmbDSG). Anders als für die öffentlichen Stellen des Bundes und vieler Länder, die zu einer Bestellung behördlicher Datenschutzbeauftragter verpflichtet sind und insoweit keinen Entscheidungsspielraum haben, stellt sich für die Hamburger Behörden die Frage des Für und Wider einer solchen Funktion. Zwar sind für diese neue Aufgabe zunächst personelle Ressourcen bereitzustellen, es stellt sich aber schnell ein direkter Vorteil für die Behörden ein, der aus der Stärkung ihrer datenschutzrechtlichen Eigenverantwortung resultiert. Ist ein behördlicher Datenschutzbeauftragter bestellt, so können die erforderlichen Verfahrensbeschreibungen und Vorabkontrollen für IT-Verfahren und Datenverarbeitungen komplett im eigenen Hause durchgeführt werden, ohne dass die ansonsten vorgesehene Einschaltung des Hamburgischen Datenschutzbeauftragten erforderlich ist. Auch die Einhaltung der Beteiligungsrichtlinie, deren unzureichende Beachtung in Einzelfällen immer wieder Anlass unserer Kritik ist, wird dadurch wesentlich erleichtert. Durch die engere Einbindung des eigenen behördlichen Datenschutzbeauftragten lassen sich diese Aufgaben effizienter und unter Wahrung behördenspezifischer Standards durchführen.

Entscheidend ist dabei, dass die erhöhte Eigenverantwortlichkeit der öffentlichen Stelle auch tatsächlich wahrgenommen werden kann. Dies setzt zum einen voraus, dass die bestellten Personen über die erforderliche Fachkunde verfügen (§ 10a Abs. 2 HmbDSG). Zum anderen ist es notwendig, dass sie in dieser Funktion ausreichend an den relevanten Verfahren beteiligt werden sowie ihr Amt aktiv ausüben können, ohne in Konflikt mit ihren sonstigen Tätigkeiten zu geraten. Dabei erweist es sich mitunter als hinderlich, dass das Hamburgische Datenschutzgesetz eine direkte Unterstellung des behördlichen Datenschutzbeauftragten unter die Behördenleitung, wie sie im Bundesdatenschutzgesetz geregelt ist, nicht vorsieht. Die Weisungsfreiheit des behördlichen Datenschutzbeauftragten steht dadurch im Spannungsverhältnis mit der Einbindung in die fachlichen Weisungsstrukturen seiner sonstigen Tätigkeit.

Um die bislang bestellten behördlichen Datenschutzbeauftragten in ihrer Stellung innerhalb ihrer Behörden zu stärken und ihre Tätigkeit zu unterstützen, haben wir ein Gesprächsforum initiiert, das den fachlichen Austausch der behördlichen Datenschutzbeauftragten untereinander sowie mit dem Hamburgischen Datenschutzbeauftragten fördert. Da die behördlichen Datenschutzbeauftragten als „Einzelkämpfer“ innerhalb ihrer sonstigen Arbeitszusammenhänge wenig Gelegenheit für fachliche Erörterungen haben, kommt einem solchen Angebot eine große Bedeutung zu. Neben der Möglichkeit, von den Erfahrungen der anderen Datenschutzbeauftragten zu profitieren oder vergleichbare Probleme gemeinsam anzugehen, ist auch die Verbesserung der Kommunikation zwischen unserer Dienststelle und den Behörden ein wichtiges Ziel dieser Initiative.

Bislang haben zwei Treffen der behördlichen Datenschutzbeauftragten stattgefunden. Eine kontinuierliche Fortsetzung ist geplant.

3. Personaldaten

3.1 Zentrum für Personaldienste (ZPD)

Bei der Einführung von Verfahren zur Verarbeitung von Mitarbeiterdaten bleibt die jeweils Daten verarbeitende Stelle datenschutzrechtlich verantwortlich. Dies gilt auch dann, wenn Dienstleistungen des ZPD in Anspruch genommen werden.

Das ZPD ist seit dem 1. Januar 2004 ein Landesbetrieb nach § 26 LHO. Als zentrale Serviceeinheit für die Freie und Hansestadt Hamburg unterstützt das ZPD die Behörden, Ämter, Landesbetriebe, Anstalten und Körperschaften in übergreifenden Angelegenheiten der Personalverwaltung. Dazu gehört die Abrechnung und Zahlung der Bezüge für rund 90.000 Beschäftigte sowie Angebote zur Beamtenversorgungs- und Ruhegeldberechnung, die Beihilfefestsetzung und die Kindergeldbearbeitung (Familienkasse). Darüber hinaus wurde das Personalcontrolling und Personalberichtswesen entwickelt, das die Steuerung von Personalstruktur und Personalkosten sowie die Personalplanung unterstützt.

Da in allen Verfahren Mitarbeiterdaten verarbeitet werden, kommt den datenschutzrechtlichen Anforderungen besondere Bedeutung zu. Zu prüfen sind insbesondere

- die jeweilige Rechtsgrundlage der Verarbeitung / Auswertungsmöglichkeiten,
- der Umfang der Daten (Erforderlichkeitsprinzip, Prinzip der Datensparsamkeit),
- die Zugriffsberechtigungen / das Berechtigungskonzept (Prinzip des „need to know“ für die jeweilige Aufgabenstellung),
- die Zulässigkeit von Datenexporten / -importen aus anderen Verfahren bzw. in andere Verfahren,
- die Aufbewahrungsfristen (Archivierungs- / Löschungskonzept).

Die Ausgestaltung der technischen und organisatorischen Maßnahmen muss sich am Schutzbedarf der Daten und den Bedrohungsszenarien (Risikoanalyse gem. § 8 Abs. 4 HmbDSG) orientieren.

Soweit das ZPD die Mitarbeiterdaten selbst als Daten verarbeitende Stelle im Sinne des Hamburgischen Datenschutzgesetzes für die ihm übertragenen Aufgaben verarbeitet (wie z. B. beim Personalberichtswesen), übernimmt der

behördliche Datenschutzbeauftragte des ZPD die wichtige Aufgabe der Vorabkontrolle.

Das ZPD bietet aber gerade die Einrichtung zentraler Anwendungen beispielsweise für die Zeitwirtschaft (siehe 3.2) und die Fortbildung (siehe 3.3) an. Bei diesen Verfahren übernimmt das ZPD zwar gewisse Dienstleistungen, die datenschutzrechtliche Verantwortung verbleibt jedoch bei den einzelnen Behörden als den Daten verarbeitenden Stellen. Diese Konstellation erhöht den nicht immer einfachen Abstimmungsaufwand für die Klärung der datenschutzrechtlichen Fragen.

3.2 SP-Expert – Zeitwirtschaftsverfahren

Mehrere, bisher separate Anwendungen werden in einem Verfahren gebündelt. Die dabei auftretenden datenschutzrechtlichen Probleme sind noch nicht abschließend gelöst.

Das Zentrum für Personaldienste (ZPD) bietet als Dienstleistung für die Behörden die Einrichtung und den Betrieb eines Zeitwirtschaftsverfahrens auf der Basis der Softwarelösung SP-Expert der Firma ASTRUM GmbH an. Das System ist modular aufgebaut und soll auf Wunsch der Kunden neben der Zeiterfassung („Kommt-Geht-Zeiten“) auch Funktionalitäten der Zeitwirtschaft (An- und Abwesenheiten, Urlaub, Krankheit) und der Personaleinsatzplanung umfassen. Eine SAP-Schnittstelle für die Kostenrechnung sowie eine Schnittstelle zum Bezügeabrechnungsverfahren PAISY für den Import von Stammdaten und die Abrechnung unständiger Bezüge ist ebenfalls vorgesehen. Ob und in welchem Umfang mit der Nutzung dieses Verfahrens Gefahren für die Rechte der betroffenen Bediensteten verbunden sind, hängt maßgeblich von den Anforderungen der jeweiligen Daten verarbeitenden Stellen an die Ausgestaltung des Verfahrens und deren Umsetzung durch das ZPD ab.

Mit der Erstellung einer Grundkonfiguration des Systems hat das ZPD u. a. folgende Anwendungen vorgesehen:

- Einrichtung permanenter, anlassunabhängiger Zugriffsrechte für Vorgesetzte auf die „Kommt-Geht-Zeiten“ ihrer Mitarbeiter.
- Festlegung der Speicherdauer für sämtliche Inhaltsdaten auf 5 Jahre.
- Bereitstellung von nicht von allen Modulen benötigten Datenfeldern.

Diese Anwendungen stoßen auf erhebliche datenschutzrechtliche Bedenken. Nach den bisherigen Darstellungen des ZPD sollen Vorgesetzten Zugriffsrechte auf die „Kommt-Geht-Zeiten“ ihrer Mitarbeiter eingeräumt werden können, wobei die Vorgesetzten ein dauerhaftes Zugriffsrecht erhalten sollen, der jeweilige Mitarbeiter keine Kenntnis über den (anlassunabhängigen) Zugriff erhält und der Zugriff nicht protokolliert wird. Sofern die Erforderlichkeit dieser

Zugriffe fachlich begründet werden kann und rechtlich zulässig ist, stellt sich die Frage nach der datenschutzgerechten Ausgestaltung des Verfahrens:

- Erfolgt eine automatische Mitteilung an den Betroffenen über den erfolgten Zugriff?
- Werden die Zugriffe protokolliert?
- Wer kontrolliert die Zugriffsprotokolle auf unberechtigte Zugriffe?

Durch die vorgesehenen Zugriffsmöglichkeiten von Vorgesetzten ergibt sich eine andere Qualität der (permanenten) Kontrolle. Die Verwaltungsanordnung über die Dienstzeit vom 18.12.96, basierend auf einer § 94er-Rahmendienstvereinbarung, sieht lediglich die stichprobenweise Kontrolle der Zeitwertkarten oder anderer Nachweise als Bestandteil der Dienstaufsicht durch die Vorgesetzten vor.

> Auszug aus den Durchführungshinweisen:
>
> „Stichprobenweise Kontrollen bedeuten die teilweise Überprüfung der Zeitwertkarten in personeller / oder zeitlicher Hinsicht. Sie kann sich auf eine Gesamtgruppe von Personen (Behörden / Amt) oder einen Gesamtzeitraum (etwa ein Jahr) beziehen. Das bedeutet, dass sowohl die Kontrolle der Zeitwertkarten eines ganzen Amtes (oder einer ganzen Abteilung) in einem bestimmten – zufällig ausgewählten – Monat als auch die Kontrolle der Zeitwertkarten eines bestimmten Personenkreises oder einer bestimmten Person Stichproben sind."

Der Pilotanwender Landesbetrieb Verkehr (LBV) sieht die Einrichtung von dauerhaften Zugriffsrechten durch die Vorgesetzten vor. Nach der Dienstvereinbarung über die Pilotphase zur Einführung eines elektronischen Zeitmanagements des LBV dient der Zugriff den Vorgesetzten zur Präsenzerfassung, zur Auswertung der Arbeitszeitkonten und für steuernde Eingriffe. Dies widerspricht den Durchführungshinweisen. Die Nutzung der technischen Möglichkeit der permanenten Kontrolle der Zeitbuchungen bzw. des Gleitzeitkontos durch die Vorgesetzten werden im LBV zwar durch eine Handlungsanweisung untersagt. Diese organisatorische Vorkehrung reicht jedoch nicht aus, denn ohne Protokollierung des lesenden Zugriffs können missbräuchliche Zugriffe im Nachhinein nicht festgestellt werden.

Da aufgrund der Art der Speicherung im System technisch eine Differenzierung der unterschiedlichen Daten in Bezug auf unterschiedliche Aufbewahrungsfristen (3 Monate bis 5 Jahre) unmöglich sei, hat das ZPD vorgesehen, die längste verbindliche Speicherfrist für alle Inhaltsdaten zu übernehmen. Die Löschungsfrist würde damit im ZPD für sämtliche Daten 5 Jahre betragen, da es sich bei einigen Inhaltsdaten um zahlungsbegründende Unterlagen im

Sinne der Landeshaushaltordnung handeln soll, für die eine Aufbewahrungsfrist von 5 Jahren gilt. Es ist derzeit ungeklärt, ob und wie das Verfahren als Kassenverfahren einzustufen ist und welche Verfahrensteile hiervon betroffen sind. Sofern eine technische Differenzierung nach unterschiedlichen Aufbewahrungszeiten nicht möglich ist, muss unabhängig davon geprüft werden, ob Daten mit unterschiedlichen Aufbewahrungszeiten überhaupt in dem gemeinsamen System verwaltet werden dürfen. Unzulässig ist nach der gegenwärtigen Rechtslage die vorgesehene Einbeziehung aller Kommt-/Geht-Zeiten sowie urlaubsbedingter und sonstiger Abwesenheit in die fünfjährige Speicherungsfrist.

Personenbezogene Daten sind zu löschen, wenn ihre Kenntnis für die Daten verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist (§ 19 Abs. 3 Nr. 2 HmbDSG). Löschen ist nach § 4 Abs. 2 Nr. 6 HmbDSG das Unkenntlichmachen von Daten oder das Vernichten des Datenträgers. Eine bestehende Löschverpflichtung kann durch eine bloße Sperrung der Daten bzw. Reduzierung der Zugriffsberechtigungen nicht ersetzt werden. Bei der Auswahl des Systems und der Konzeption des Verfahrens müssen entsprechende rechtliche Rahmenbedingungen und Vorgaben berücksichtigt werden. Das ZPD teilte mit, dass derzeit ein Löschungskonzept erarbeitet werde.

Um bei der Bündelung unterschiedlicher Anwendungen dem Datenschutz Rechnung zu tragen, soll ein Genehmigungsworkflow eingerichtet werden. Dabei ist zu berücksichtigen, dass

- festgelegt wird, wer welche Schreib- und Leserechte für welche Daten sowie für welchen Zweck und Zeitraum hat,
- die Authentizität der Antrags- und Bewilligungsdaten gewährleistet wird,
- die aktuellen Genehmigungsinstanzen eingepflegt sind.

Als Benutzerkennung ist die Personalnummer vorgesehen. Dies würde eine Zweckänderung der Personalnummer bedeuten, da die Nutzung für Identifizierungszwecke in der geltenden § 94er Vereinbarung Propers nicht vorgesehen ist. Durch die Verwendung der Personalnummer als Benutzerkennung würde diese wie eine sonstige Nutzerkennung auch im Zusammenhang mit Anmeldungs- und Abmeldungsprozessen protokolliert (Zugriff durch Administratoren).

Daneben wurde festgestellt, dass nicht benötigte Felder softwareseitig nicht gesperrt werden können. Als Lösung käme gegenwärtig nur in Betracht, diese Felder beim regelmäßigen Datenexport aus PAISY als „leer“ zu überschreiben. Dies widerspricht dem Prinzip der Datenvermeidung und -sparsamkeit, da eine manuelle Dateneingabe dennoch nicht verhindert wird.

Das ZPD beabsichtigt, für die Anwendung von SP-Expert eine § 94er-Rahmendienstvereinbarung abzuschließen, deren Verhandlungen wir aus datenschutzrechtlicher Sicht begleiten werden. Bis dahin darf eine Anwendung nur

im Umfang der geltenden Dienstvereinbarung erfolgen. Darüber hinaus werden wir die Gespräche mit dem ZPD fortsetzen, um eine datenschutzgerechte Lösung der noch offenen Fragen zu erreichen. Die Daten verarbeitenden Stellen haben zu gewährleisten, dass SP-Expert nur in dem gegenwärtig zulässigen Rahmen eingesetzt wird.

3.3 CLIX – Zentrale Fortbildung

Mit der Einrichtung des Zentrums für Aus- und Fortbildung verändert sich die Seminarverwaltung. Die dabei auftretenden datenschutzrechtlichen Probleme sind noch nicht abschließend geklärt.

Das Zentrum für Aus- und Fortbildung (ZAF) plant und verwaltet Seminarangebote für alle Angehörigen des Öffentlichen Dienstes in Hamburg. Die bisher zur Unterstützung dieser Aufgabe eingesetzte Software wird durch die Standardsoftware CLIX (Corporate Learning & Information eXchange) abgelöst. Die Einführung ist in vier Stufen vorgesehen, in denen Daten unterschiedlicher Vertraulichkeit verarbeitet oder veröffentlicht werden:

- Stufe 1 (1. Juli 2005):
  Planung und Erstellung des Fortbildungsangebotes
- Stufe 2 (voraussichtlich Mitte Januar 2006):
  Möglichkeit der Online-Anmeldung zu Fortbildungsveranstaltungen für die Beschäftigten einschließlich der elektronischen Unterstützung der nötigen behördlichen Genehmigungs- und Mitbestimmungsverfahren.
- Stufe 3 (voraussichtlich I. Halbjahr 2006):
  Aufbau eines E-Learning-Portals für die Durchführung der Fortbildung zu den Microsoft-Office-Produkten.
- Stufe 4 (voraussichtlich II. Halbjahr 2006):
  Berechnung des geldwerten Vorteils.

Daten verarbeitende Stelle ist das ZAF, Dienstleister sind jeweils ZPD für die Anwendung und Dataport für die technische Realisierung.

Durch die Online-Anmeldung (Stufe 2) erhalten die Beschäftigten die Möglichkeit, direkt aus dem Online-Katalog Seminare auszuwählen und sich für diese Seminare anzumelden. Jede Anmeldung startet einen Genehmigungsworkflow. Zur Vereinfachung der Anmeldung und zur Erhöhung der Datenqualität war bisher geplant, die notwendigen Daten regelmäßig aus dem Hamburg Service Informationssystem (HaSI) und dem Personalabrechnungsverfahren PAISY zu importieren. Für diesen Import ist jedoch eine Rechtsverordnung notwendig, die derzeit von der Finanzbehörde vorbereitet wird. Solange der Senat diese Rechtsverordnung nicht beschlossen hat, dürfen keine Daten aus anderen Systemen zu CLIX importiert werden. Für die Benutzer von CLIX bedeutet dies, dass sie sich einmalig beim ZAF anmelden und dann alle persönlichen

Daten manuell eingeben. Weiterhin müssen die Benutzer diese Daten regelmäßig auf aktuellem Stand halten.

Daneben besteht für alle Mitarbeiter die Möglichkeit, sich wie bisher formularmäßig anzumelden. Die Daten werden dann von den Mitarbeitern des ZAF erfasst.

Mit der Einführung der Online-Anmeldung bei Veranstaltungen im Verwaltungsseminar Kupferhof e.V. sollten auch Daten an den Kupferhof zur Organisation der Übernachtung übergeben werden. Der direkte Zugriff von Mitarbeitern des Kupferhofs auf diese Daten ist jedoch gegenwärtig unzulässig. Der Kupferhof ist als eingetragener Verein eine nicht öffentliche Stelle, ungeachtet der Beteiligung durch die FHH (§ 2 Abs. 1 Satz 2 HmbDSG). Das Einräumen einer Zugriffsberechtigung stellt einen automatisierten Abruf dar. Ein automatisiertes Verfahren zum Abruf personenbezogener Daten durch Dritte darf nur eingerichtet werden, wenn eine Rechtsvorschrift dies ausdrücklich zulässt (§ 11 Abs. 1 HmbDSG). Das Verfahren muss daher so gestaltet werden, dass keine Zugriffsberechtigung für den Kupferhof eingerichtet wird. Die personenbezogenen Daten der Teilnehmer dürfen jedoch vom ZAF an den Kupferhof übermittelt werden.

Für die Personalentwickler der jeweiligen Behörden, die im Verhältnis zum ZAF als Daten verarbeitende Stelle Dritte sind, ist ein lesender Zugriff auf die Kurshistorie vorgesehen. Die insoweit bestehenden datenschutzrechtlichen Fragen werden mit dem Personalamt erörtert.

Die Dauer der Speicherung der Kurshistorie konnte noch nicht abschließend geklärt werden. Derzeit sind 5 Jahre vorgesehen.

3.4 PIA – Projekt interner Arbeitsmarkt

Die datenschutzrechtlichen Anforderungen sind wegen der Sensibilität der personenbezogenen Daten hoch.

PIA soll im Sinne einer Personalberatungs- und Vermittlungsagentur folgende Aufgaben erfüllen:

- Analyse des internen und externen Arbeitsmarktes, einschließlich der Überwachung des restriktiven Einstellungsverfahrens.
- Beratung von Beschäftigten und Behörden in allen Fragen der individuellen und strukturellen Mobilität.
- Qualifizierung der Beschäftigten, Vorbereitung auf neue Aufgaben.
- Vermittlung von Beschäftigten in neue Aufgabenfelder.
- Aktive Erschließung neuer Aufgabenfelder, die im Einzelfall auch außerhalb der hamburgischen Verwaltung liegen können.
- Unterstützung bei der Aufnahme selbstständiger Tätigkeit.

- Entwicklung von Instrumenten, die zur Verbesserung der Steuerung des internen Arbeitsmarktes dienen und dessen Transparenz erhöhen.

Die Beschäftigungsbehörden erstellen mittels eines Fragebogens, der mit dem Hamburgischen Datenschutzbeauftragten abgestimmt wurde, erste Kompetenzprofile in Zusammenarbeit mit den von strukturellen Veränderungen betroffenen Beschäftigten (strukturelle Mobilität) und übermitteln diese Profile an PIA. Auch können sich Mitarbeiterinnen und Mitarbeiter aus eigener Initiative mit einem Veränderungswunsch an PIA wenden (individuelle Mobilität). Zudem ist PIA für die Stellenausschreibungen der FHH zuständig.

PIA hat sich zur Datenverarbeitung für eine externe ASP (Application Service Provider)-Lösung auf Basis einer webbasierten Applikation entschieden. Da es sich um sensible Mitarbeiterdaten handelt, sind die dafür notwendigen datenschutzrechtlichen Anforderungen zu erfüllen. Neben der Festlegung der technischen und organisatorischen Maßnahmen gegenüber dem Auftragnehmer waren folgende Vorkehrungen zu treffen:

- Sicherer Transportweg zum Auftragnehmer (verschlüsselt).
- Administrationskonzept (Ausschluss des Zugriffs auf die Datenbank durch externe Administratoren).
- Berechtigungskonzept (nur PIA-Mitarbeiter haben Zugriff auf die Datenbank).
- Sichere Authentifizierung der Nutzer (Client-Zertifizierung).
- Keine personenbezogene Kommunikation mit den Beschäftigten über das Internet.

Nach der § 94er-Rahmendienstvereinbarung Bürokommunikation, Anlage E-Mail-Nutzung, dürfen sensible personenbezogene Daten elektronisch nur verschlüsselt übermittelt werden. Innerhalb des FHHinfoNET ist dies durch die in Outlook bereitgestellte Funktionalität „Erweiterte Sicherheit“ grundsätzlich möglich (vgl. 18. TB, 11.1). PIA hat dazu in Abstimmung mit dem Hamburgischen Datenschutzbeauftragten eine Liste erstellt, welche Inhalte unverschlüsselt gesendet werden können und welche nur verschlüsselt übermittelt werden dürfen.

4. Statistik

4.1 Datenübermittlung zur Durchführung von Schulstatistiken

Für die Übermittlung von individuellen statistischen Schüler- und Lehrerdaten und deren Verarbeitung in einer länderübergreifenden Datenbank sind entsprechende Rechtsvorschriften zu schaffen.

Das Statistische Amt für Hamburg und Schleswig-Holstein hat die Behörde für Bildung und Sport (BBS) aufgefordert, Einzeldatensätze aus dem Verwaltungsvollzug zur Durchführung von Schulstatistiken zu übermitteln. Dabei hat sich das Statistische Landesamt auf entsprechende Beschlüsse der Kultusministerkonferenz (KMK) vom Mai 2003 und Vereinbarungen der KMK mit den Statistischen Landesämtern berufen, nach denen schulstatistische Individualdaten im Umfang eines festgelegten Kerndatensatzes („Kerndatensatz für schulstatistische Individualdaten der Länder“) übermittelt werden sollen.

Bei diesen Einzeldatensätzen handelt es sich nicht um Geschäftsstatistiken im Sinne des § 8 Hamburgisches Statistikgesetz (HmbStatG), sondern um Landesstatistiken. Hierzu bedarf es nach § 2 Abs. 1 HmbStatG einer Rechtsnorm, in der insbesondere der Kreis der Betroffenen, die Hilfs- und Erhebungsmerkmale, die Art der Erhebung, der Berichtszeitraum, der Berichtszeitpunkt und bei wiederkehrenden Erhebungen deren zeitliche Abstände zu bestimmen sind. Da das Hamburgische Schulgesetz (HmbSG) keine entsprechende Regelung enthält, haben wir die BBS und das Statistische Amt für Hamburg und Schleswig-Holstein darauf hingewiesen, dass eine solche Schulstatistik nicht ohne entsprechende Rechtsgrundlage (z. B. im HmbSG) durchgeführt werden darf. Nach Mitteilung des Statistischen Amtes für Hamburg und Schleswig-Holstein sind von der BBS bislang keine Individualdaten, sondern lediglich aggregierte Daten, die keinen Personenbezug zulassen, übermittelt worden.

Aus den Vorbemerkungen des uns vorliegenden Entwurfs des Kerndatensatzes (KDS) der Länder für schulstatistische Individualdaten des Sekretariats der Kultusministerkonferenz vom 28. Februar 2005 geht weiterhin hervor, dass der KDS in einer gemeinsamen Datenbank der Länder geführt werden soll und für die „Koordinierung politischer und planerischer Maßnahmen sowie für die internationale Zusammenarbeit auf dem Gebiet des Schulwesens“ als unerlässlich angesehen wird.

Dies ist auf die Amtschefkonferenz der KMK vom 8. Mai 2003 in Fulda zurückzuführen, wonach unter TOP 16 beschlossen wurde, dass die Länder vereinbaren, bei der Umstellung der Schulstatistik auf Individualdaten einen sog. Kerndatensatz zu verarbeiten und alle 16 Bundesländer ihre Daten zwecks Verbesserung der „überregionalen Bildungsberichterstattung“ in eine gemeinsame Datenbank einspeisen. Die Einrichtung der gemeinsamen Datenbank soll unter den statistischen Ämtern des Bundes und der Länder ausgeschrieben werden.

Die Einstellung der Datensätze in eine gemeinsame Datenbank stößt auf erhebliche datenschutzrechtliche Bedenken, weil es sich hierbei um eine bundesweite Zusammenfassung von pseudonymisierten Schüler- und Lehrerdaten handelt, die in den Kompetenzbereich der Länder fällt und für deren Verarbeitung eine entsprechende länderübergreifende Rechtsgrundlage zu schaffen ist. Wir haben daher die BBS gebeten, auf der nächsten KMK auf die

Schaffung einer entsprechenden Rechtsgrundlage (z. B. Staatsvertrag zwischen den Bundesländern) hinzuwirken.

Entwürfe für die beiden zu schaffenden Rechtsgrundlagen lagen uns bei Redaktionsschluss noch nicht vor. Daher bleibt die Fortentwicklung dieses Vorhabens abzuwarten.

4.2 Erfassung betreuter Personen für die Kinder- und Jugendhilfestatistik

Die Erhebung von Adressdaten betroffener Personen ist nur auf der Grundlage einer besonderen Rechtsnorm zulässig. Die zur Identifizierung von Betroffenen dienenden Merkmale sind zu anonymisieren.

Mehrere öffentliche und nicht-öffentliche Stellen der Erziehungsberatung haben sich an uns gewandt, weil vom Statistischen Amt für Hamburg und Schleswig-Holstein neue Erhebungsbögen für die Statistik der Kinder- und Jugendhilfe eingesetzt werden, mit denen erstmals auch die Adressen der betreuten Personen erfasst werden sollen. Mitarbeiterinnen und Mitarbeiter der Beratungsstellen befürchten, dass dadurch die Anonymität der Betreuten nicht mehr sichergestellt werden könne, und bezweifeln die Erforderlichkeit der Adressdaten.

Unsere Prüfung hat ergeben, dass mit dem Erhebungsbogen der Kinder- und Jugendhilfestatistik Teil I (Institutionelle Beratung) erstmals ab dem Berichtsjahr 2004 das statistische Erhebungsmerkmal „Blockseite“ erhoben wird, um für kleinräumige (sozial-räumliche) Planungszwecke regionalisierte Informationen über Lebenslagen, Sozialisationsbedürfnisse, Handlungspotential und Defizitlagen von Kindern, Jugendlichen und ihren Familien zu erhalten.

Rechtsgrundlagen für diese Erhebung bilden die §§ 98 bis 103 Sozialgesetzbuch VIII (SGB VIII) in Verbindung mit § 23 Hamburgisches Gesetz zur Ausführung des SGB VIII (AG SGB VIII) vom 25. Juni 1997 (HmbGVBl. S. 273). Danach wird für die Kinder- und Jugendhilfestatistik in Hamburg neben den bisherigen Erhebungsdaten auch das Erhebungsmerkmal „Blockseite“ erhoben (§ 23 Abs. 1 AG SGB VIII). Dieses Merkmal ist nach dem Bundesstatistikgesetz (BStatG) die kleinste regional definierte statistische Ergebniseinheit und zugleich die tiefste Aggregationsstufe für regional gegliederte statistische Einzeldatensätze. Als Hilfsmerkmal zum Merkmal „Blockseite“ ist die Anschrift (Straße, Hausnummer) der betreuten Kinder, Jugendlichen und jungen Volljährigen bestimmt worden (§ 23 Abs. 2 AG SGB VIII). Diese Angaben werden im Statistischen Amt mit Hilfe eines speziell gefertigten Programms zu Blockseiten verschlüsselt, so dass bei der Auswertung statt der Anschrift nur noch ein numerischer Wert angezeigt wird.

Die Erhebung von Anschriften der betreuten Personen beruht somit auf einer bereichsspezifischen Rechtsgrundlage und steht im Einklang mit den Vorschriften des Datenschutzes. Sie ist insoweit datenschutzrechtlich zulässig.

Die Prüfung des Erhebungsbogens hat jedoch ergeben, dass eine physikalische Trennung von Hilfs- und Erhebungsmerkmalen (z. B. durch Abtrennen) nicht möglich war, weil sich die Hilfsmerkmale zur Ermittlung der Blockseite sowie die Erhebungsmerkmale auf der Vorder- und Rückseite eines Blattes befanden. Wir haben daher das Statistische Amt auf das gesetzliche Trennungsgebot des § 12 BStatG hingewiesen. Danach sind die Hilfsmerkmale (Adressdaten) von den Erhebungsmerkmalen zum frühestmöglichen Zeitpunkt zu trennen und zu löschen. Das Statistische Amt hat daraufhin alle auskunftspflichtigen Stellen durch ein Rundschreiben auf dieses Problem hinweisen und die mit uns abgestimmte Maßnahme zum Trennen beim Rücklauf der bereits versandten Erhebungsbogen erläutert. Zur Gewährleistung der gesetzlich gebotenen Trennung von Erhebungs- und Hilfsmerkmalen haben wir vereinbart, dass die betreffenden Seiten der Erhebungsbögen nach Eingang auf verschiedene Einzelblätter kopiert werden, damit die Erhebungs- und Hilfsmerkmale jeweils auf separaten Blättern vorliegen und getrennt behandelt werden können. Damit konnte den Anforderungen des § 12 BStatG Rechnung getragen werden.

5. Finanzen und Steuern

Authentifizierung bei der elektronischen Steuererklärung ELSTER

Bei der elektronischen Übermittlung von Steuererklärungsdaten muss eine Identifizierung des Absenders gewährleistet werden.

Seit dem 1. Januar 2005 haben Unternehmer dem Finanzamt ihre Umsatzsteuervoranmeldungen und Lohnsteueranmeldungen nach amtlich vorgeschriebenem Vordruck nur noch auf elektronischem Wege nach Maßgabe der Steuerdaten-Übermittlungsverordnung (StDÜV) zu übermitteln. Voraussetzung hierfür sind ein Internetzugang und eine für die Datenübermittlung geeignete Software. Der Fiskus stellt hierfür das kostenlose Programm ELSTER (elektronische Steuererklärung) zur Verfügung.

Durch Eingaben und Presseberichte sind wir auf Manipulationsmöglichkeiten bei der elektronischen Übermittlung von Steuererklärungsdaten mit der Steuersoftware ELSTER aufmerksam geworden. Dabei wurde insbesondere beklagt, dass bei diesem Verfahren keine Prüfung der Absenderidentifizierung vorgenommen wird und ein Dritter für die Manipulation einer Steueranmeldung neben dem Namen eines Unternehmers lediglich dessen Steuernummer benötigt. Die Steuernummer könne jedoch problemlos jeder Rechnung des betreffenden Unternehmers entnommen werden. Da solch ein Verfahren nicht akzeptiert werden kann, haben wir die Finanzbehörde um entsprechende Stellungnahme gebeten. Wegen der bundesweiten Tragweite dieser Sicherheitsproblematik hat sich neben anderen Landesdatenschutzbeauftragten auch der Bundesbeauftragte für den Datenschutz des Themas angenommen.

Die Finanzbehörde und das Bundesministerium der Finanzen vertreten dazu die Auffassung, dass die Manipulationsanfälligkeit des Steueranmeldungsverfahrens nicht auf dem Verfahren ELSTER beruhe, sondern Folge der geltenden Rechtslage sei. Dabei werde das Risiko einer unbefugten Erklärungsabgabe oder unberechtigten Erstattung (auch zugunsten Dritter) als gering angesehen, weil die Betrugsmöglichkeiten durch entsprechende Sicherheitsmaßnahmen (z. B. maschinelle Plausibilitätskontrollen, Risiko-Management) im Festsetzungsverfahren eingeschränkt würden. Hierzu wurden allerdings keine weiteren Einzelheiten genannt. Unzutreffende Steueranmeldungen werden jedoch in der Regel erst nach der Datenverarbeitung, insbesondere aufgrund von Einwendungen des Steuerpflichtigen, erkannt. Dies gelte aber gleichermaßen für elektronisch übermittelte wie für herkömmliche Steueranmeldungen.

Eine sichere Authentifizierung durch den Einsatz einer qualifizierten elektronischen Signatur hätte gemäß § 87a Abs. 3 Satz 2 Abgabenordnung (AO) gewährleistet werden können. Hierauf hat die Finanzverwaltung jedoch verzichtet, um den angestrebten zügigen Aufbau der elektronischen Kommunikation zwischen den Steuerpflichtigen und der Finanzverwaltung nicht zu behindern. Stattdessen wurde die Übergangsbestimmung des § 87a Abs. 6 AO genutzt, nach der bis zum 31. Dezember 2005 eine „qualifizierte elektronische Signatur mit Einschränkungen“ eingesetzt werden kann. Hiergegen hat sich bereits die 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003 in ihrer Entschließung „Elektronische Signatur im Finanzbereich“ ausgesprochen und die qualifizierte elektronische Signatur gefordert. Nunmehr soll ein geeignetes Authentifizierungsverfahren im Jahre 2006 bundesweit zum Einsatz kommen. Dieses Verfahren wird seit einigen Monaten in mehreren Ländern (darunter Bayern, Hessen, Nordrhein-Westfalen und Sachsen) pilotiert. Ergebnisse der Pilotierung lagen bei Redaktionsschluss jedoch noch nicht vor.

6. Personenstandswesen

Übertragung von Eheschließungen im Internet

Das Angebot eines Standesamtes, Eheschließungen per Webcam ins Internet zu übertragen, muss den Anforderungen des Datenschutzes entsprechen.

Das Standesamt Hamburg-Wandsbek beabsichtigt anzubieten, dass auf Wunsch des Brautpaares die Eheschließung „live“ in das Internet übertragen werden kann, damit Verwandte, Freunde und Bekannte, die nicht anwesend sind, virtuell an der Eheschließung teilnehmen können.

Geplant ist, die Eheschließung mit zwei Webcams ohne Ton aufzunehmen und in das Internet zu übertragen. Die „Live"-Aufnahmen sollen dann über einen begrenzten Zeitraum im Internet zugänglich sein. Auf Wunsch soll die Eheschließung auch vorher im sog. „Digitalen Hochzeitskalender" angekündigt werden können. Dazu sollen die Vornamen und ein gemeinsames Porträtfoto der Brautleute im Internet veröffentlicht werden. Weiterhin ist vorgesehen, ein Bild der Eheschließenden fünf Jahre in einem Hochzeitsarchiv zu speichern.

Ob es zur Aufgabe des Staates gehört, seiner Kundenorientierung dadurch zu entsprechen, dass ein solches Internetangebot zur Verfügung gestellt wird, wird von uns sehr kritisch gesehen. Unseres Erachtens sollte es genügen, auf Wunsch der Eheschließenden private Videoaufnahmen von der Eheschließung zuzulassen unter der Bedingung, dass alle Beteiligten ausdrücklich zustimmen. Sollte das Standesamt jedoch die Verantwortung dafür übernehmen wollen, dass es die Eheschließung ins Internet stellt, müssen von ihm die nachstehenden datenschutzrechtlichen Voraussetzungen erfüllt werden:

- Die Übertragung der Eheschließung in das Internet stellt eine Datenübermittlung nach § 4 Abs. 2 Nr. 4 des Hamburgischen Datenschutzgesetzes (HmbDSG) dar. Mangels einer bereichsspezifischen Rechtsvorschrift, die eine derartige Veröffentlichung erlaubt, ist dies nur zulässig, wenn die Betroffenen darin eingewilligt haben (§ 5 Abs. 1 Nr. 2 HmbDSG). Zugleich ist das „Recht am eigenen Bild" berührt, so dass für die „Live"-Aufnahmen und deren Übertragung in das Internet auch insoweit eine Einwilligung der Betroffenen erforderlich ist. Die betroffenen Personen, das Brautpaar, die Trauzeugen, geladene Verwandte, Bekannte und Gäste sowie die Bediensteten des Standesamtes, können nur dann rechtswirksam in die Übertragung einwilligen, wenn sie zuvor umfassend über die Veröffentlichung im Internet und deren Folgen informiert werden (§ 5 Abs. 2 HmbDSG). Die Betroffenen sind auch darüber zu informieren, dass die erstellten Bilder weltweit einsehbar sind und durch Dritte gespeichert, manipuliert und für andere Zwecke verwendet werden können.
- Zuständig für die Information der Betroffenen und die Einholung der Einwilligung ist die Daten erhebende und übermittelnde Stelle, somit das Standesamt Hamburg-Wandsbek. Die Unterrichtung kann nicht dem Brautpaar überlassen werden.
- Für das Brautpaar und die betroffenen Bediensteten des Standesamtes ist eine schriftliche Einwilligung unverzichtbar. In der Einwilligungserklärung des Brautpaares hat dieses zu bestätigen, dass es ihre Trauzeugen und die Hochzeitsgesellschaft vorab über die beabsichtigte Internetübertragung informiert, damit diese bei der Trauung nicht davon überrascht werden.

- Da der Kreis der übrigen Personen (z. B. Verwandte, Freunde, Bekannte) vorher nicht immer feststeht und sich auch kurzfristig noch ändern könnte, muss die Information dieser Personen auch dadurch sichergestellt werden, dass im Wartezimmer der Hochzeitsgäste entsprechende Informationsblätter ausgelegt werden und auch an der Tür des Trauzimmers auf die Internetübertragung aufmerksam gemacht wird. Weiterhin sind die bei der Trauung anwesenden Personen vor der Einschaltung der Webcams nochmals durch die Standesbeamtin oder den Standesbeamten über den Wunsch des Brautpaares und die Folgen der Internetübertragung zu informieren. Nehmen die so informierten Personen dann an der Eheschließung teil, haben sie konkludent eingewilligt. Die Standesbeamtin oder der Standesbeamte hat die Unterrichtung der Betroffenen in der Trauungsverfügung schriftlich zu dokumentieren.
- Sofern einzelne Personen mit der Übertragung nicht einverstanden sind, ist sicherzustellen, dass diese Personen nicht von den Webcams erfasst werden. Ihnen ist ein aufnahmefreier Platz im Trauungsraum zuzuweisen.
- Der Zugriff auf die „Live"-Aufnahmen im Internet sollte zeitlich beschränkt werden und hat sich am Grundsatz der Erforderlichkeit zu orientieren. Wenn eine Eheschließung „live" über das Internet mitverfolgt werden soll, so genügt in der Regel ein Übertragungszeitraum, der durch die Dauer der Trauungszeremonie bestimmt wird. Eine darüber hinausgehende zeitliche Zugriffsmöglichkeit könnte dem Brautpaar selbst überlassen bleiben. Hierfür erscheint eine Speicherung von 14 Tagen angemessen zu sein. Dabei könnten die Aufnahmen auch in einem ausschließlich für das Brautpaar zugänglichen Archiv (nur zugänglich mit Benutzerkennung und Password) gespeichert werden. So kann das Brautpaar dann weitgehend selbst bestimmen, wie die Aufnahmen weiterverwendet werden und wer die Aufnahmen erhalten soll. Auf diese Weise könnten einer unkontrollierbaren Fremdnutzung von vornherein Grenzen gesetzt werden.
- Die endgültige Fassung der schriftlichen Einwilligungserklärungen sowie des Informationsblattes und Hinweisschildes sind dem Hamburgischen Datenschutzbeauftragten vor der Aufnahme des Echtbetriebes zur abschließenden Stellungnahme zuzuleiten.

Das Standesamt Hamburg-Wandsbek hat erklärt, es werde ein datenschutzkonformes Verfahren implementieren. Die Abstimmung der Einwilligungserklärung und Informationshinweise ist inzwischen weitgehend abgeschlossen. Wann mit der Aufnahme des Echtbetriebes zu rechnen ist, liegt noch nicht fest. Es wurde vereinbart, dass wir zuvor prüfen können, ob das konkrete Vorhaben in Übereinstimmung mit dem Datenschutz steht.

7. Polizei

7.1 Novellierung des Polizeirechts

Die neuen Instrumente der Polizei für verdachtsunabhängige Vorfeldermittlungen greifen massiv in das Grundrecht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung und Schutz der Privatsphäre ein.

Am 29. Juni 2005 ist das Zweite Gesetz zur Änderung des Gesetzes über die Datenverarbeitung der Polizei in Kraft getreten. Mit diesem Gesetz wurden neue Eingriffsbefugnisse für die Polizei geschaffen, die weit über das klassische Feld der polizeilichen Tätigkeit hinausgehen. Die datenschutzrechtliche Problematik dieser Instrumente liegt darin, dass zum Tätigwerden der Polizei nicht mehr eine konkrete Gefahr oder ein Anfangsverdacht für die Begehung einer Straftat vorliegen muss, sondern die Polizei bereits weit im Vorfeld einer Gefahrenlage und möglicher künftiger Straftaten tätig werden kann. Durch diese Maßnahmen, die im Wesentlichen in der Erhebung, der Speicherung und im Abgleich personenbezogener Daten bestehen, werden zwangsläufig überwiegend völlig unbeteiligte und rechtstreue Bürger in die Beobachtung und Datenerfassung durch die Polizei einbezogen. Diese Verdachtsschöpfungsinstrumente greifen tief in den Persönlichkeits- und Datenschutz gänzlich unverdächtiger Bürger ein.

Wir haben daher im Gesetzgebungsverfahren gefordert, dass die Befugnis der Polizei zu diesen neuen Datenerhebungen strikten rechtsstaatlichen Begrenzungen unterliegen muss. In dieser Forderung sehen wir uns durch das Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 zur präventiven Telekommunikationsüberwachung nach niedersächsischem Polizeirecht (vgl. 7.2) bestätigt.

Die neuen gesetzlichen Vorschriften zur Durchführung verdachtsunabhängiger Personenkontrollen und zur Videoüberwachung an öffentlich zugänglichen Orten setzen für das polizeiliche Eingreifen keinen konkreten Anlass oder Verdacht voraus. Eine Beschränkung dieser Maßnahmen auf Bereiche, die ein deutlich überproportionales Aufkommen an Straßenkriminalität erkennen lassen und sich damit als Kriminalitätsbrennpunkte erweisen, kann zumindest dem Gesetzeswortlaut nicht entnommen werden. Wir werden sorgfältig darauf achten, dass die neuen Instrumente in der polizeilichen Praxis mit Augenmaß angewandt werden.

Die Behörde für Inneres (BfI) hat angekündigt, im ersten Quartal 2006 mit der Videoüberwachung der Reeperbahn zu beginnen. Die Behörde verweist dabei auf die im Vergleich zu anderen Orten mit Abstand höchste Kriminalitätsbelastung insbesondere bei Gewaltdelikten und auf die Gefahr der Eskalation von Auseinandersetzungen unter Alkohol- und Drogeneinfluss. Die eingesetzten schwenkbaren Kameras sollen mit einer Zoom-Funktion ausgestattet sein

und Bilder live in die Polizeieinsatzzentrale senden. Eine Erfassung privater, der staatlichen Beobachtung nicht zugänglicher Bereiche soll durch eine Programmierung der Kameras ausgeschlossen werden. Die Einstufung der Reeperbahn als Kriminalitätsbrennpunkt können wir nachvollziehen. Die Aufzeichnung, Speicherung und Auswertung der Videobilder werden wir überprüfen.

Das Gesetz lässt die Überwachung und Aufzeichnung von Telekommunikation zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person zu. Die Maßnahme ist unter einen grundsätzlichen Richtervorbehalt gestellt und speziellen Regelungen zum Schutz der Kommunikation mit engsten Vertrauten und Berufsgeheimnisträgern unterworfen. Ob diese Regelungen entsprechend den Vorgaben des Urteils des Bundesverfassungsgerichts vom 27. Juli 2005 (vgl. 7.2) noch verbessert werden müssen, bedarf der Prüfung. Wir begrüßen, dass der Gesetzgeber dem Entwurf des Senats insoweit nicht gefolgt ist, als dieser eine weitergehende präventive Telekommunikationsüberwachung vorsah.

Die Bürgerschaft hat unsere Anregung aufgegriffen, im Polizeirecht eine besondere Rechtsgrundlage für Datenübermittlungen an nicht-öffentliche Stellen im Rahmen von Zuverlässigkeitsüberprüfungen aus Anlass gefährdeter Veranstaltungen zu schaffen. Einen bedeutsamen Anwendungsfall dieser Regelung bildet das am 3. Oktober 2005 eingeleitete Akkreditierungsverfahren für die Fußball-WM 2006 (vgl. 7.3). Die Vorschrift erlaubt allerdings nur einen Abgleich mit polizeilichen Dateien. Eine Anfrage an das Ausländerzentralregister (AZR) kann darauf nicht gestützt werden.

7.2 Präventive Telekommunikationsüberwachung

Das Bundesverfassungsgericht hat in seinem Urteil vom 27. Juli 2005 hohe rechtsstaatliche Hürden für verdeckte polizeiliche Vorfeldermittlungen errichtet.

Das Bundesverfassungsgericht hat die Vorschriften des niedersächsischen Polizeirechts zur präventiven Telekommunikationsüberwachung wegen Unvereinbarkeit mit dem Grundrecht auf Brief-, Post- und Fernmeldegeheimnis für nichtig erklärt. Nach Auffassung des Gerichts darf der Landesgesetzgeber zwar Bestimmungen zur vorbeugenden Bekämpfung von Straftaten als Teil der Gefahrenabwehr erlassen. Ihm fehlt jedoch die Kompetenz für Regelungen, die der Vorsorge für die Verfolgung noch nicht begangener Straftaten dienen. Das Gericht hat darüber hinaus Verstöße des Gesetzgebers gegen die Grundsätze der Normenklarheit und der Verhältnismäßigkeit gerügt. Dabei hat es die prognostischen Unwägbarkeiten und die große Streubreite der Vorfeldermittlungen sowie die vielseitige Verwendbarkeit der daraus gewonnenen personenbezogenen Erkenntnisse berücksichtigt. Ferner hat das Gericht die fehlenden Vorkehrungen des Gesetzgebers zum Schutz des unantastbaren Kernbereichs privater Lebensgestaltung beanstandet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom 27./28. Oktober 2005 die Gesetzgeber in Bund und Ländern aufgerufen, aus dem Urteil des Bundesverfassungsgerichts Konsequenzen für alle verdeckten Ermittlungsmethoden auf den Gebieten der Gefahrenabwehr und der Strafverfolgung zu ziehen. Insbesondere wurde gefordert, dass dem verfassungsrechtlich absolut geschützten Kernbereich privater Lebensgestaltung nicht nur durch Verwendungsverbote und Löschungspflichten, sondern durch Untersagungen bereits im Stadium der Datenerhebung wirksam Rechnung getragen werden müsse.

Praktische Bedeutung könnte die Forderung der Datenschutzbeauftragten für den verdeckten Einsatz technischer Mittel außerhalb von Wohnungen, insbesondere in Kraftfahrzeugen, erlangen. Die Anwendung des besonderen Kernbereichsschutzes auf diese Fallgestaltung hatte das Bundesverfassungsgericht bislang nicht zu entscheiden. Da das Kraftfahrzeug nicht nur Fortbewegungsmittel, sondern vielfach auch Ort privater Kommunikation zwischen engsten Vertrauten ist, sprechen gewichtige Gründe für seine Einbeziehung in den Kernbereichsschutz.

7.3 Akkreditierungsverfahren Fußball WM 2006 (Beteiligung Verfassungsschutz)

Das Akkreditierungsverfahren weist gravierende datenschutzrechtliche Defizite auf.

Am 3. Oktober 2005 hat das Akkreditierungsverfahren des Deutschen Fußball-Bundes e.V. (FIFA Fußball-Weltmeisterschaft 2006 Organisationskomitee Deutschland – OK WM 2006) für die Fußball-WM 2006 (9. Juni bis 9. Juli 2006) begonnen. Durch dieses Verfahren soll der Zutritt zu den Spielstätten, z. B. zum Spielfeld, zum Umkleide- und VIP-Bereich sowie zum Medienzentrum, geregelt werden. Von der Akkreditierung betroffen sind ca. 250.000 Personen. Im Einzelnen umfasst dieser Personenkreis Mitarbeiter der FIFA und des OK WM 2006, Angehörige der Mannschaften und Begleitdelegationen, Mitarbeiter und Berechtigte der offiziellen Partner des Veranstalters, Medienvertreter sowie Personen, die im Bereich Sicherheit und durch Hilfsdienste eingesetzt werden können, einschließlich Polizeibeamte, Freiwillige und Servicebedienstete aller Sparten.

Akkreditiert werden darf nur, wer sich ohne negatives Gesamtvotum der beteiligten Sicherheitsbehörden (Polizei, Verfassungsschutz) einer Zuverlässigkeitsüberprüfung unterzogen hat. Die Überprüfung erfolgt anhand der Datensätze, die das OK WM 2006 zentral dem Bundeskriminalamt (BKA) zur Verfügung stellt und die von dort an die für den Wohnort der Betroffenen zuständigen Landeskriminalämter weitergeleitet werden. Die Daten werden mit verschiedenen polizeilichen Dateien abgeglichen, z. B. mit den Staatsschutzdateien und mit der Gewalttäterdatei Sport. Nach der Meldedatenüber-

mittlungsverordnung (MDÜV) darf die Polizei zur Identitätsprüfung der Betroffenen auch einen Abgleich mit Meldedaten (Familienname, Vorname, frühere Namen, Geburtsdatum, Anschrift) im automatisierten Abrufverfahren (EWO-Abfrage) durchführen. Ferner werden die Daten vom BKA an das Bundesamt für Verfassungsschutz (BfV) übermittelt. Dort erfolgt eine automatisierte Abfrage über das Nachrichtendienstliche Informationssystem (NADIS). Aktenhinweise in NADIS werden bei der zuständigen Landesverfassungsschutzbehörde überprüft und ausgewertet. Dies gilt auch für Erkenntnisse, die als Verschlusssache (VS) eingestuft sind oder dem Quellenschutz unterliegen. Polizei und Verfassungsschutz nehmen jeweils eine Einzelfallprüfung vor und fügen ihre Einschätzungen zu einem Gesamtvotum zusammen. Nach Abschluss der Überprüfung teilt das BKA dem OK WM 2006 das Ergebnis mit, ob Zuverlässigkeitsbedenken bestehen oder nicht. Welche Dienststelle Bedenken geltend gemacht hat und worauf sich die Bedenken im Einzelnen stützen, erfährt das OK WM 2006 nicht.

Gegen das Akkreditierungsverfahren haben wir deutliche Kritik erhoben. Wir teilen nicht die Auffassung des Veranstalters und der meisten Sicherheitsbehörden, dass eine Einwilligungserklärung der Betroffenen auf der Grundlage einer ausführlichen Datenschutzinformation zur rechtlichen Absicherung des Akkreditierungsverfahrens ausreicht. Ob und in welchem Umfang personenbezogene Erkenntnisse, die vielfach verdeckt mit besonderen Erhebungsmethoden gewonnen wurden und einer engen gesetzlichen Zweckbindung unterliegen, für den vorbeugenden, verdachtsunabhängigen Schutz einer privat organisierten Veranstaltung genutzt werden dürfen, hat allein der demokratisch legitimierte Gesetzgeber zu entscheiden. Ferner ist zu bedenken, dass die Betroffenen häufig zur Sicherung ihrer beruflichen Existenz auf eine Akkreditierung angewiesen sind und daher nicht frei wählen können, ob sie die Einwilligung erteilen oder verweigern.

Die Bürgerschaft hat unsere Anregung aufgegriffen und die unverzichtbare gesetzliche Grundlage für einen polizeilichen Datenabgleich im Rahmen von Zuverlässigkeitsüberprüfungen aus Anlass besonders gefährdeter privater Veranstaltungen geschaffen (vgl. 7.1). Dem Landesamt für Verfassungsschutz (LfV) haben wir dringend empfohlen, eine entsprechende gesetzliche Regelung auch für den nachrichtendienstlichen Bereich zu initiieren. Der Verfassungsschutz ist in gleicher Weise auf Rechtssicherheit und klare, gerichtsfeste Überprüfungsmaßstäbe angewiesen wie die Polizei. Das LfV hält demgegenüber die Einwilligungslösung für recht- und zweckmäßig. Diese Einschätzung wird vom Innenausschuss der Bürgerschaft geteilt.

Bedenken gegen das Akkreditierungsverfahren ergeben sich ferner im Hinblick auf den Grundsatz der Verhältnismäßigkeit. Wir halten es auch unter Berücksichtigung von Sicherheitsaspekten für unangemessen, 250.000 Personen im Wege der verdachtsunabhängigen Regelanfrage beim Verfassungs-

schutz einem NADIS-Abgleich zu unterziehen. Bei den zu akkreditierenden Personen handelt es sich weder um exponierte Geheimnisträger noch um Beschäftigte in sicherheitsempfindlicher Funktion, von denen ein Sabotage- oder Anschlagsrisiko für lebens- und verteidigungswichtige Einrichtungen ausgeht. Erkenntnisse über terroristische oder andere politisch motivierte Gewalttaten liegen in aller Regel auch beim Staatsschutz vor und werden deshalb bereits im Rahmen des polizeilichen Datenabgleichs erfasst. Nicht nachvollziehen können wir, dass – wie der Datenschutzinformation zu entnehmen ist – darüber hinaus auch tatsächliche Anhaltspunkte für Propagandaaktivitäten ein ablehnendes Votum des Verfassungsschutzes rechtfertigen sollen. Dies führt in erheblichem Umfang zur Einbeziehung gewaltfreier, nicht strafbarer Verhaltensweisen oder entsprechender Ankündigungen. Damit entfernt sich das Akkreditierungsverfahren deutlich von seiner Zweckbestimmung, die Sicherheit der Veranstaltung im Sinne eines präventiven Rechtsgüterschutzes zu gewährleisten.

8. Justiz

8.1 Weitere Neuregelungen der DNA-Analyse im Strafverfahren

Der erneut erweiterte Anwendungsbereich der DNA-Analyse lässt befürchten, dass der Gesetzgeber solange weiteren Handlungsbedarf sieht, bis die Gleichsetzung mit dem herkömmlichen Fingerabdruck erreicht ist. Die gesetzliche Regelung des Reihengentests ist zu begrüßen.

Am 1. November 2005 ist das Gesetz zur Novellierung der forensischen DNA-Analyse in Kraft getreten (BGBl. Teil I, 2360), mit dem der Anwendungsbereich der DNA-Analyse wiederum erweitert wurde. Im Wesentlichen handelt es sich um folgende Änderungen:

- Für die molekulargenetische Untersuchung von Körperzellen eines noch nicht bekannten Spurenlegers entfällt die richterliche Anordnung ebenso wie bei schriftlicher Einwilligung des Beschuldigten sowohl zur Beweisführung im anhängigen Ermittlungsverfahren als auch zur Beweisführung in künftigen Strafverfahren.
- Für die Beweisführung in künftigen Strafverfahren entfallen die bisher in § 81g Abs. 1 Nr.1 Strafprozessordnung (StP0) aufgezählten Regelbeispiele. Die DNA-Analyse wird erstreckt auf wiederholt begangene oder wiederholt zu begehende sonstige Straftaten, die jeweils für sich betrachtet, die Schwelle der Erheblichkeit nicht erreichen, in ihrer Gesamtheit aber einer Straftat von erheblicher Bedeutung gleichstehen.
- Erstmals wird der Reihengentest (das sog. DNA-Massenscreening) gesetzlich mit dem in die Strafprozessordnung eingefügten § 81h geregelt; nach einer vorherigen richterlichen Anordnung können auf freiwilliger Basis nun

von Personen, die bestimmte auf den bis dato unbekannten Täter vermutlich zutreffende Merkmale erfüllen, Körperzellen entnommen und molekulargenetisch untersucht und (nur) mit tatrelevantem Spurenmaterial abgeglichen werden. Eine andere oder weitere Verwendung der Testdaten ist unzulässig.

Der Wegfall des Erfordernisses einer richterlichen Anordnung für den Fall, dass Spurenmaterial eines noch nicht bekannten Spurenlegers zu untersuchen ist, ist datenschutzrechtlich nicht zu beanstanden.

Grundsätzlich verfassungsrechtlich unbedenklich ist auch der Wegfall des Richtervorbehalts, wenn der Betroffene in die molekulargenetische Untersuchung seiner Körperzellen einwilligt. Es obliegt dem Betroffenen, über seine Grundrechte der körperlichen Unversehrtheit und der informationellen Selbstbestimmung selbst zu verfügen. Gefahren liegen aber in der Art und Weise der gesetzlich vorgeschriebenen Belehrung. Damit von dem Betroffenen wirksam in den Grundrechtseingriff eingewilligt werden kann, ist er im Rahmen einer qualifizierten Belehrung einzelfallbezogen über den Zweck der Datenerhebung wie auch über die weitere Nutzung sowie über die Dauer der Speicherung aufzuklären. Im Rahmen der schriftlichen Belehrung müssen daher zumindest die Hinweise erfolgen, dass

- die gesetzlichen Voraussetzungen für eine richterliche Anordnung vorliegen,
- die Einwilligung eine Speicherung des DNA-Musters in der entsprechenden Datei des Bundeskriminalamtes zur Folge hat,
- der Datensatz des Betroffenen künftig regelmäßig zu einem verdachtsunabhängigen Abgleich mit Tatortspuren verwendet werden kann.

Aus einer unzureichenden Belehrung können sich in einem späteren Strafverfahren Beweisverwertungsprobleme ergeben. Die sich aus der DNA-Analyse im Strafverfahren ergebenden Vorteile würden dann ins Leere verlaufen.

Die Erweiterung der materiellen Voraussetzungen der DNA-Analyse für künftige Strafverfahren ist mit Blick auf die zahlreichen unbestimmten Rechtsbegriffe in § 81 g Abs. 1 Satz 2 StP0 zumindest als zweifelhaft einzustufen. Unklar bleibt, ob sich überhaupt Straftaten aus dem mittleren Bereich oder gar aus dem Bereich der Bagatellkriminalität finden lassen, die die Schwelle zur Erheblichkeit nur deshalb überschreiten, weil sie wiederholt begangen werden. Abzulehnen ist auch, dass Anlasstaten für die Beurteilung mit zu berücksichtigen sind, die nur „begangen“, aber noch nicht rechtskräftig abgeurteilt wurden, insoweit also der schlichte Verdacht ausreicht. Was passiert, wenn ein Teil der berücksichtigten, bisher nur begangenen Taten nicht zu einer rechtskräftigen Verurteilung führt, die Daten aber bereits eingestellt sind? Wird dann eine erneute Prüfung sichergestellt? Als problematisch ist auch zu bewerten, dass mit der jetzigen Regelung die schriftliche Begründung der Gefahrenprognose,

für die das Bundesverfassungsgericht wegen der Schwere des Grundrechtseingriffs konkrete Vorgaben gemacht hat, im Falle einer Einwilligung entfällt. Es erscheint daher sinnvoll, wenigstens von der Staatsanwaltschaft eine schriftliche Fixierung der unterschiedlichen Aspekte zu fordern, zumal dies im Falle einer verweigerten Einwilligung sowieso erforderlich wird.

Datenschutzrechtlich zu begrüßen ist die Benachrichtigungspflicht des Bundeskriminalamtes in den Fällen, in denen ein für ein Ermittlungsverfahren gemäß § 81 e StP0 gewonnenen DNA-Identifizierungsmuster in die dort geführte Datei eingestellt worden ist. Die Rechte des Betroffenen werden dadurch gewahrt, dass die Benachrichtigung mit dem Hinweis zu verbinden ist, dass gegen die Einstellung in die Datei die gerichtliche Entscheidung beantragt werden kann und damit Rechtsschutz gewährt wird.

Die gesetzliche Regelung der Reihengentests verdient Zustimmung, weil nun klargestellt ist, unter welchen Voraussetzungen eine solche Untersuchung stattfinden darf. Da die gewonnenen Daten unverzüglich zu vernichten sind, wenn feststeht, dass die untersuchte Person als Spurenleger ausscheidet, und die Speicherung der Daten in der DNA-Analyse-Datei des Bundeskriminalamtes sowie auch ein Abgleich mit dort bereits gespeicherten Daten unzulässig ist, bestehen aus datenschutzrechtlicher Sicht keine Bedenken. Zumal auch kein Anfangsverdacht im Sinne von § 152 StP0 begründet wird, wenn eine der zum Test gebetenen Personen die freiwillige Mitwirkung verweigert. In einem solchen Fall müssen neben der Weigerung weitere konkrete verdachtsbegründende Umstände hinzukommen, die dann eine Anordnung nach §§ 81 e, 81 f StP0 begründen können.

8.2 Zentralarchiv und Zentralkartei der Justizvollzugsanstalt Fuhlsbüttel

Im Bereich des Zentralarchivs haben sich datenschutzrechtliche Defizite gezeigt, die den Anforderungen an einen Schutz der besonders sensiblen Daten in keiner Weise gerecht wurden. Als Hausarbeiter im Zentralarchiv eingesetzte Gefangene hatten Zugriffsmöglichkeiten auf personenbezogene Daten entlassener Gefangener. Mit der Aufarbeitung der Problembereiche konnte eine Sensibilisierung der zuständigen Behörden für datenschutzrechtliche Belange erreicht werden.

Aufgrund einer Eingabe wurde zunächst bekannt, dass ein im Zentralarchiv der JVA Fuhlsbüttel von April 2004 bis Juni 2005 mit Archivierungsarbeiten beschäftigter Gefangener ungehinderten und unbeaufsichtigten Zugang zu den dort archivierten Gefangenenpersonalakten (GPA) hatte. Der Aufgabenbereich des Gefangenen umfasste das Anlegen von Karteikarten, die Ablage von gerichtlichen Schreiben, Haftersuchen, Anträgen von verschiedenen anderen Behörden – u. a. der Staatsanwaltschaft – durch Einsortieren in die GPA, die Bearbeitung der Zugangslisten aus der Untersuchungshaftanstalt in der

Weise, dass er die entsprechenden GPA aus früheren Aufenthalten der Gefangenen heraussuchte. Im Ergebnis nahm der Gefangene hochsensible personenbezogene Daten früherer Gefangener wahr. Das Strafvollzugsamt hat diesen Sachverhalt bestätigt und einen Verstoß gegen die Verwaltungsvorschrift Nr. 5 zu § 37 Strafvollzugsgesetz eingeräumt, zunächst aber darauf verwiesen, dass lediglich eine „einzelfallspezifische Fehlleistung einzelner Mitarbeiter auf Arbeitsebene" vorliege, die dadurch angemessen aufgearbeitet worden sei, dass diese Praxis eingestellt und der eingerichtete Gefangenenarbeitsplatz ersatzlos gestrichen wurde.

In der folgenden Zeit stellte sich – unter anderem durch eine datenschutzrechtliche Prüfung – heraus, dass

- weitere vier Gefangene im Zeitraum von Juli 2002 bis April 2004 im Zentralarchiv als Hausarbeiter mit Reinigungs-, aber auch mit Archivierungsaufgaben sowie mit dem Transport von Gefangenenpersonalakten befasst waren;
- im Zentralarchiv wegen räumlicher Unterbringungsprobleme in der Vollzugsgeschäftsstelle auch Teilbände von Gefangenenpersonalakten von 28 aktuell einsitzenden Gefangenen offen eingelagert waren, zu denen sich die dort beschäftigten Hausarbeiter unbeaufsichtigten Zugang verschaffen konnten;
- einer der Hausarbeiter sich in einem Fall Kenntnis aus einer Gefangenenpersonalakte darüber verschaffen konnte, dass dieser betroffene Gefangene mit den Ermittlungsbehörden zusammen gearbeitet hatte und deswegen im Zeugenschutzprogramm gewesen war;
- auf den Gefangenenpersonalakten bzw. den Karteikarten Hinweise auf die Zugehörigkeit zum Zeugenschutzprogramm verzeichnet waren, so dass die als Hausarbeiter eingesetzten Gefangenen sich z. T. als „streng vertraulich" bezeichnete Daten hätten verschaffen können;
- eine Fristenkontrolle der an andere Behörden oder Justizvollzugsanstalten versandten Gefangenenpersonalakten fehlte;
- in einer automatisierten Datei, die von den Mitarbeitern, die die „Zentralkartei" verwalten, geführt wird, auf die aber auch die Mitarbeiter des Zentralarchivs wie der Vollzugsgeschäftsstelle Zugriff hatten, über einen einfachen Filter auf eine „Unterdatei" zugegriffen werden konnte, die die Namen der Gefangenen enthielt, die sich im Zeugenschutzprogramm befunden haben, wobei diese „Unterdatei" längere Zeit nicht aktualisiert worden war.

Durch die im Ergebnis konstruktive Zusammenarbeit mit dem Strafvollzugsamt sowie auch der Leitungsebene der Justizvollzugsanstalt Fuhlsbüttel konnten Lösungen entwickelt werden, die nach ihrer Umsetzung die Wahrung des Datenschutzes in diesem Bereich gewährleisten werden. So sind für die im Zentralarchiv eingelagerten Personalakten der aktuell einsitzenden Gefange-

nen verschließbare Aktenstahlschränke angeschafft worden, die so im Bereich des Zentralarchivs aufgestellt wurden, dass einerseits die Mitarbeiter der Vollzugsgeschäftsstelle keinen Zugriff die auf archivierten Gefangenenpersonalakten und andererseits die Mitarbeiter des Zentralarchivs keinen Zugriff mehr auf die aktuellen Gefangenenpersonalakten haben. Den Voraussetzungen des § 183 Strafvollzugsgesetz ist damit Genüge getan. Im Rahmen einer klaren schriftlichen Dienstanweisung werden die Akten- und Zugriffstrennung geregelt wie auch die administrative Handhabung der besonders sensiblen, personenbezogenen Daten derjenigen Gefangenen, die im Zeugenschutzprogramm waren oder sind, ferner die Rücklauf- wie Fristenkontrolle von an andere Dienststellen herausgegebene Gefangenenpersonalakten. Hausarbeiter erhalten keinen Zugang mehr zum Zentralarchiv. Vorübergehend haben die Mitarbeiter des Zentralarchivs die Reinigungsarbeiten übernommen. Künftig werden diese Arbeiten Reinigungskräfte einer Fremdfirma ausführen, die nach dem Hamburgischen Sicherheitsüberprüfungsgesetz vor Beginn ihrer Tätigkeit auf Zuverlässigkeit überprüft werden.

9. Behördlicher Aktentransport

In erheblichem Umfang wurden Datenschutzverstöße sowie Verletzungen des Sozial- und Steuergeheimnisses beim Post- und Aktenaustausch durch die offene Versendung von Gerichtsakten und anderen personenbezogenen Vorgängen in Betreuungs-, Familien- und Strafsachen sowie Sozialleistungsangelegenheiten festgestellt.

Da Kontrollen beim Behörden-Transport-Service (BTS) in den Vorjahren gravierende Verletzungen des Datenschutzes ergeben hatten (vgl. 17. TB, 18; 18. TB, 5.2; 19. TB, 14.2), wurden die Kontrollen im Berichtszeitraum fortgesetzt.

Einen Schwerpunkt der Feststellungen bildete dabei erneut die Justiz. Bei Datenschutzkontrollen im September / Oktober 2005 wurden beim BTS in größerer Anzahl Betreuungsbeschlüsse und in Einzelfällen auch vollständige Betreuungsakten vorgefunden, die von der Geschäftsstelle des Amtsgerichts Hamburg offen ohne Umschlag an die Betreuungsstelle Nord der Behörde für Soziales und Familie (BSF) oder an das Klinikum Nord übersandt wurden. Das Spektrum schwerer Krankheiten, die aus den Unterlagen personenbezogen nachvollzogen werden konnten, umfasst Psychosen, Demenz, Intelligenzminderung, Linseninfarkt und Hepatitis C. Ferner konnte beim BTS eine Anfrage des Amtsgerichts Hamburg an das Staatsarchiv eingesehen werden, die einen namentlich konkret bezeichneten Adoptionsfall betraf. In einer Familiensache wurde dem Jugendamt unverschlossen die Stellungnahme eines Suchtberaters übermittelt. Wir haben die Problematik eingehend mit dem Präsidenten

des Amtsgerichts Hamburg erörtert. Uns wurde zugesagt, die gerichtsinternen Stichprobenkontrollen zu intensivieren.

Auch andere Stellen der Justiz legten nicht die erforderliche Sorgfalt beim Post- und Aktenaustausch an den Tag. Offen vorgefunden wurden beim BTS Bewährungs- und Strafvollstreckungshefte, Entlassungsmitteilungen von Justizvollzugsanstalten, eine Kindergeldakte, bereits ausgefüllte Fragebögen zum Versorgungsausgleich, Unterlagen aus Verfahren über das Umgangsrecht und die Erlaubnis zur Eheschließung zwischen Minderjährigen, die fachärztliche Diagnose einer depressiven Störung sowie die Bescheinigung einer gesetzlichen Krankenkasse über Arbeitsunfähigkeitszeiten mit Angaben zur Heroinabhängigkeit.

In Einzelfällen erhielten wir von den datenschutzrechtlich verantwortlichen Stellen kurzfristig Abhilfemitteilungen, die sich bei späteren Kontrollen des BTS auch bestätigten. So trug das Justizverwaltungsamt der Justizbehörde dafür Sorge, dass Zahlungsanzeigen über die Einzahlung von Bußgeld auf das Treuhandkonto „Sammelfonds für Bußgelder“ nur noch in verschlossenen Umschlägen an das zuständige Finanzamt gelangen. Das Strafvollzugsamt wies die Vollzugsgeschäftsstellen an, Mitteilungen über Straf- und Untersuchungsgefangene nur in verschlossenen Umschlägen zu versenden. Ein gemeinnütziges Wohnungsbauunternehmen ist unserer dringenden Empfehlung gefolgt und übersendet die Abschriften fristloser Kündigungen wegen Zahlungsverzuges nunmehr verschlossen an die Bezirksstelle zur Wohnungssicherung.

Von verschiedenen Finanzämtern wurden Vorgänge, die Steuergeheimnisse enthielten, offen versandt. So fanden wir beim BTS Schriftsätze des Finanzamtes Hamburg-Mitte an das Finanzgericht Hamburg unverschlossen vor und konnten Einblick in die beigefügten Einkommensteuer-, Gewerbesteuer-, Umsatzsteuer-, Arbeitgeber-, Betriebsprüfungs- und Rechtsbehelfsakten nehmen. Wir haben hierzu eine Stellungnahme des Finanzamtes Hamburg-Mitte eingeholt und gemeinsam mit dem Vorsteher und Geschäftsstellenleiter des Finanzamtes die Verfahrensabläufe in der Aktenaustauschstelle überprüft, die der Steuerverwaltung der Finanzbehörde unterstellt ist. Darüber hinaus unterrichteten wir die Steuerverwaltung auch unmittelbar über festgestellte Datenschutzverstöße im Bereich der Finanzämter. Dies gilt für unverschlossene Mitteilungen in Gewerbeuntersagungsverfahren und Verfahren nach dem Bundesausbildungsförderungsgesetz so wie für die offene Übersendung eines Haftbefehls zur Erzwingung der Abgabe einer eidesstattlichen Versicherung. Wir hoffen, dass das Steuergeheimnis künftig durch verschlossenen Aktenversand gewahrt wird.

Schließlich stellten wir fest, dass das Sozialgeheimnis im Berichtszeitraum teilweise massiv verletzt wurde. Die datenschutzrechtliche Verantwortung hierfür liegt bei einzelnen Grundsicherungs- und Sozialdienststellen der Bezirke sowie bei der Hamburger Arbeitsgemeinschaft SGB II (ARGE), die über die

Gewährung von Arbeitslosengeld II bzw. Sozialgeld zu entscheiden hat. Leistungsakten und einzelne Unterlagen der ARGE fanden wir sowohl beim BTS als auch in der Poststelle des Bezirksamts Hamburg-Mitte offen vor. Zur Kenntnis gelangten auf diese Weise ein fachchirurgisches Gutachten, die Arbeitsunfähigkeitsbescheinigung eines Nervenarztes, die Bescheinigungen von Internisten über das Vorliegen einer HIV-Infektion, die Mitteilung, dass das Ärztegremium einem Blinden die Erwerbsunfähigkeit bescheinigt habe, Hinweise auf Leistungsmissbrauch, der Kostenfestsetzungsbescheid einer Wohnunterkunft für Obdachlose, Nachweise über Trainingsmaßnahmen und Vermittlungsbemühungen sowie Auskunftsersuchen in Einbürgerungsverfahren. In einem Gespräch mit Vertretern der ARGE wurden strukturelle Problemlösungen entwickelt. Das technisch-organisatorische Konzept der ARGE beinhaltet eine Agenturweisung zur Postabfertigung, die Benennung der für den Datenschutz persönlich Verantwortlichen bei den einzelnen Standorten, klare und einheitliche Vorgaben für die Auszeichnung von Postsendungen sowie die Verwendung spezieller Postversandtaschen und Verschlussaufkleber. Auch in dem Entwurf einer Dienstanweisung zur Anlage, Führung und Vernichtung von SGB II-Leistungsakten, den die ARGE gegenwärtig mit uns abstimmt, wird der verschlossene behördeninterne Postversand ausdrücklich vorgeschrieben. Die Anforderungen der ARGE an den Datenschutz wurden in enger Abstimmung mit dem Leiter des BTS definiert und werden regelmäßig in Gesprächsrunden der Standortleiter erörtert. Diese konstruktiven Bemühungen tragen dem hohen Schutzniveau der Sozial- und Gesundheitsdaten angemessen Rechnung.

10. Gewerbe und Umwelt

10.1 Begutachtung der wirtschaftlichen Lage des Taxigewerbes

Die Erhebung sensibler personen- und unternehmensbezogener Daten eines Dienstleistungsgewerbes erfordert umfangreiche Datenschutzmaßnahmen.

Die für die Durchführung des Personenbeförderungsgesetzes (PBefG) zuständige Behörde für Stadtentwicklung und Umwelt (BSU) hat ein privates Institut mit der Erstellung eines Gutachtens beauftragt, um die wirtschaftliche Lage des Hamburger Taxengewerbes präzise beurteilen und einschätzen zu können. Dazu ist eine umfangreiche Datenerhebung bei den Taxenunternehmen erforderlich, da die der Behörde bisher vorliegenden Erkenntnisse ausschließlich auf Angaben einzelner Gewerbevertreter und allgemeinen statistischen Daten beruhen. Zugleich soll geprüft werden, ob durch die Einführung von „Fiskaltaxametern“ Missbrauchs- und Umgehungstatbestände beim Betrieb von Taxen verringert werden können.

Die für die Begutachtung erforderlichen Daten sollen über einen Zeitraum von drei Jahren erhoben werden. Hierbei hat der Gutachter gemäß vertraglicher Vereinbarung mit der BSU das Hamburgische Datenschutzgesetz (HmbDSG) anzuwenden. Vor Beginn der Datenerhebung war für das Gesamtprojekt u. a. eine Risikoanalyse zu erstellen und der BSU ein mit dem Hamburgischen Datenschutzbeauftragten abgestimmtes Datenschutzkonzept vorzulegen.

Die erforderlichen Daten sollen durch zwei Erhebungsmethoden gewonnen werden:

- Erhebung steuer- und betrieblicher Daten: Die Daten zur Bewertung der betriebswirtschaftlichen und betrieblichen Situation der Hamburger Taxenunternehmen werden zunächst auf der Grundlage des § 54a PBefG schriftlich mittels Fragebogen erhoben. Von dieser Aktion sind insgesamt ca. 770 Taxenunternehmen betroffen, wobei alle Mehrwagenunternehmen teilnehmen und von den Einwagenunternehmen eine repräsentative Zufallsstichprobe gezogen wurde. Für die betroffenen Taxenunternehmer besteht eine Auskunftspflicht.
- Erhebung von Daten zu Umsatz und Einsatzzeit der Taxen: Die Erhebung dieser betriebswirtschaftlichen Daten erfolgt mit Hilfe von Taxametern. Neuere Modelle werden auch „Fiskaltaxameter“ genannt. Hierbei handelt es sich um Fahrpreisanzeiger bzw. Wegstreckenzähler, die das komplette Fahrgeschehen, das Fahrpersonal sowie die Einnahmen langfristig und auslesbar speichern. Diese Daten zu Umsätzen und Einsatzzeiten werden dabei mittels spezieller Datenträger – so genannten „Keys“ – ausgelesen. Dieses Verfahren ist bereits bei vielen Mehrwagenunternehmen im Einsatz und kommt dem Konzept des „Fiskaltaxameters“ nahe. Da der Einsatz von sog. „Fiskaltaxametern“ in Deutschland gesetzlich nicht geregelt ist, kann die Rekrutierung der Teilnehmer nur auf freiwilliger Basis durchgeführt werden. Für die Erhebung wurde ein „Fiskaltaxameter“-Panel von ca. 160 Taxifahrzeugen gebildet.

Die Auslesung der Daten wird an dezentralen sog. Sample Points durchgeführt. Hierbei handelt es sich um wichtige Frequenzpunkte des Taxengewerbes, wie z. B. bestimmte Tankstellen, Fachwerkstätten oder Funkzentralen. Am Sample Point ist ein Key-Lesegerät vorhanden, dass als Peripheriegerät an einen lokalen, zugriffsgesicherten Rechner angeschlossen ist. Die hier vom Fahrer mittels Key ausgelesenen Daten werden auf der Festplatte des Rechners zwischengespeichert. Als Bestätigung erhält der Fahrer einen Quittungsausdruck.

Neben den dezentralen Sample Points wird ein zentraler Administrationspunkt eingerichtet. Hier werden die dezentral gesammelten Daten der Panel-Fahrzeuge per ISDN-Verbindung gesammelt, aufbereitet und in Fahrzeug-Konten erfasst. Am Administrationspunkt erfolgt die statistische Auswertung und die gutachterliche Bewertung der Daten.

In Abstimmung mit uns wurden in dem Datenschutzkonzept insbesondere folgende datenschutzrechtlichen Festlegungen getroffen:

- Die betroffenen Unternehmen und teilnehmenden Fahrer haben ihre Einwilligungen zur Erhebung mittels Taxameter schriftlich zu erteilen. In der Einwilligungserklärung sind Zweck und Umfang der Datenverarbeitung, Art der Daten, Adressaten der Übermittlung, Dauer der Aufbewahrung und die Rechtsfolgen bei Verweigerung und Widerruf der Einwilligung zu regeln.
- Bei der Erhebung werden keine Namen von Fahrern erfasst, sondern nur Unternehmer- und Fahrzeugdaten. Fahrgastbezogene Daten werden nicht erhoben. Da auch die sensiblen unternehmensbezogenen Daten (z. B. Umsätze, Einsatzzeiten) zu schützen sind, wird für diese der gleiche Maßstab wie für personenbezogene Daten angelegt. Direkt nach dem Einlesen am Sample Point werden die Daten, die Rückschlüsse auf den Fahrer zulassen, automatisch pseudonymisiert und gleichzeitig verschlüsselt. Nach der Prüfung auf Plausibilität, Integrität, Authentizität und Kontinuität der Daten werden sämtliche Merkmale, durch die eine Person bestimmbar gemacht werden kann, anonymisiert. Anschließend werden die nicht mehr benötigten Daten mit Unternehmensbezug gelöscht.
- Die Auslesegeräte an den Sample Points stehen unter ständiger Aufsicht des Tankstellen- bzw. Funkzentralenpersonals, so dass eine Manipulation oder ein Diebstahl schnell bemerkt werden kann. Als weiterer Schutz werden die Rechner verplombt. Der Zugriff erfolgt über die Passwortsicherung gemäß der hamburgischen Passwortrichtlinie. Als weitere Schutzmaßnahme werden die eingelesenen Daten verschlüsselt gespeichert. Die Auslesung und Löschung der Daten erfolgt durch den Gutachter in der Regel werktäglich. Die zentrale Auslesung ist nur durch Eingabe einer geheimen ISDN-Einwahlnummer möglich. Eine Verbindung kann ausschließlich mit der ISDN-Kennung des Servers am Administrationspunkt erfolgen, so dass mit einer abweichenden ISDN-Kennung keine Datenverbindung aufgebaut werden kann.
- Der zentrale Administrationspunkt befindet sich in den Geschäftsräumen des Gutachters. Zugriff über ein Passwort haben nur die Mitarbeiter, die mit dem Projekt betraut sind. Wartungsarbeiten durch den Softwarehersteller erfolgen nur unter Kontrolle des betrieblichen Datenschutzbeauftragten des Gutachters. Mögliche Eingriffe in die Programmabläufe werden protokolliert. Durch eine umfassende Dokumentation wird gewährleistet, dass Fehler in der Programmlogik ohne Zugriff auf die originale Datenbasis gesucht und gefunden werden können.

Vor Beginn der Datenerhebung mittels „Fiskaltaxameter“ haben wir uns im Rahmen einer Vorführung davon überzeugt, dass die im Datenschutzkonzept getroffenen Festlegungen eingehalten worden sind. Eine nachgehende datenschutzrechtliche Kontrolle ist vorgesehen.

10.2 Kundendatei und Prüfungen von Heizöltanks

Die Übermittlung von personenbezogenen Daten ist nur nach den Grundsätzen des Datenschutzes zulässig.

Durch mehrere Eingaben haben wir davon Kenntnis erhalten, dass die regelmäßige Prüfung von Heizöltanks nach der Verordnung zum Umgang mit wassergefährdenden Stoffen und über Fachbetriebe (Anlagenverordnung – VAwS) vom 19. Mai 1998 (HmbGVBl. S. 71) nicht mehr von der zuständigen Behörde, sondern von einer privaten Sachverständigenorganisation (SVO) durchführt wird.

Die Betroffenen wurden durch ein Schreiben der privaten SVO darüber informiert, dass sie mit ihrer Heizöllagerbehälteranlage nunmehr in der Kundendatei der SVO geführt werden und dass die Überprüfung ihrer Anlage fällig sei. Anderen Schreiben der SVO sowie der Behörde für Wissenschaft und Gesundheit – Amt für Gesundheit und Verbraucherschutz (früher: Amt für Arbeitsschutz – AfA – der ehemaligen Behörde für Arbeit und Gesundheit) war zu entnehmen, dass die bisher staatlich wahrgenommene Aufgabe nunmehr auf der Grundlage einer Kooperationsvereinbarung auf die SVO übertragen wurde und fällige Prüftermine künftig mit der SVO zu vereinbaren sind.

Die betroffenen Betreiber waren verunsichert und beklagten insbesondere, dass die Datenübermittlung von der Behörde an die private SVO ohne ihre Zustimmung erfolgte und mit den Anschreiben der SVO der Anschein einer behördlich vorgeschriebenen Übernahme durch die private SVO erweckt wurde und somit eine Wahlmöglichkeit hinsichtlich der Inanspruchnahme anderer SVO nicht bestehe.

Unsere Prüfung hat zu folgendem Ergebnis geführt: Nach dem Wegfall des Sachverständigenmonopols auf dem Gebiet des Wasserrechts im Jahre 1998 erhielt das Amt für Arbeitsschutz (AfA) gemäß § 22 VAwS für die Dauer von fünf Jahren die Anerkennung als Sachverständigenorganisation (SVO). Für diese Aufgabenerfüllung betrieb das AfA eine umfangreiche Datenbank, in welcher u. a. auch die privaten Heizöllagerbehälter und deren Betreiber gespeichert waren. Wer seine Heizölbehälteranlage nach dem Wasserrecht prüfen lassen wollte, konnte sich also noch bis zum 31. Dezember 2003 an das Amt für Gesundheit und Verbraucherschutz als Nachfolgerin des AfA wenden.

Der am 31. Dezember 2003 auslaufende Anerkennungsbescheid nach § 22 VAwS wurde nicht neu beantragt. Die bei der Behörde tätigen Sachverständigen führten ihre VAwS-Prüfungen auf Grund einer offiziellen Benennung durch die private SVO fort. Zur Sicherung der Arbeitsplätze der noch tätigen Sachverständigen wurde mit dieser SVO ein Kooperationsvertrag geschlossen und ihr die VAwS-Daten sämtlicher Anlagen übermittelt. Dabei soll es sich um ca. 14.000 Datensätze gehandelt haben. Die Prüfung des Kooperationsvertrages

hat jedoch ergeben, dass die Übertragung der VAwS-Prüfaufgaben auf die private SVO ohne formelle Aufgabenübertragung stattgefunden hat.

Nach § 5 Abs. 1 Hamburgisches Datenschutzgesetz (HmbDSG) ist die Verarbeitung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift über den Datenschutz sie erlaubt oder die Betroffenen eingewilligt haben. Da nach unseren Feststellungen keine dieser Voraussetzungen für die Übermittlung der Datensätze aus dem „VAwS-Bereich" an die private SVO vorgelegen hat, sind die Datensätze in unzulässiger Weise an die SVO übermittelt worden.

Aus diesem Grund haben wir die SVO aufgefordert, die übermittelten Datensätze in ihrem DV-System gemäß § 35 Bundesdatenschutzgesetz (BDSG) unverzüglich und vollständig zu löschen und keinen anderen Zwecken zuzuführen. Hierüber haben wir die Behörde für Stadtentwicklung und Umwelt als zuständige Aufsichtsbehörde nach dem Wasserrecht informiert.

Bei der Löschung war jedoch zu beachten, dass die personenbezogenen Daten bei der privaten SVO in Form von Kundenadressen gespeichert und verarbeitet werden. Da einem Kunden aber nicht nur ein Heizöllagerbehälter, sondern auch andere Objekte (z. B. Aufzug, Kraftfahrzeug) zugeordnet sein konnten, würden im Falle der Löschung des Kunden auch die rechtsgültigen Daten zu den anderen Objekten gelöscht werden. Es musste daher bei der SVO zunächst in jedem Einzelfall geprüft werden, ob ein Kunde nicht in Zusammenhang mit anderen Objekten oder Vorgängen steht, die möglicherweise in anderen Geschäftsbereichen der SVO bearbeitet wurden oder werden. Diese Einzelfallprüfung gestaltete sich sehr zeitaufwändig, so dass die VAwS-Daten bis zur Löschung für jede weitere Nutzung zu sperren waren. Nur wenn festgestellt wurde, dass ein Kunde keinem anderen Objekt als einem Heizöllagerbehälter zugeordnet konnte, war eine Löschung angezeigt.

Führte der Heizöllagerbehälter jedoch zu einem Kunden, dem noch andere Objekte zugeordnet werden konnten, so durfte lediglich das Objekt Heizöllagerbehälter gelöscht werden; der Kunde selbst musste für die anderen Rechtsbezüge weiter gespeichert bleiben.

Zu beachten war auch, dass die VAwS-Datensätze von juristischen Personen grundsätzlich nicht dem Schutz des HmbDSG bzw. BDSG unterliegen und somit nicht zu löschen waren. Personenbezogene Daten durften ferner dann nicht gelöscht werden, wenn sie beispielsweise aus Gründen der Buchführungspflicht weiterhin aufzubewahren waren oder die Kunden zuvor in diese Prüfung eingewilligt hatten.

Im Rahmen einer nachgehenden Kontrolle haben wir an Hand von 20 Adressen prüfungspflichtiger Heizöllagerbehälteranlagen im DV-System der privaten SVO stichprobenartige Suchläufe durchgeführt. Das Ergebnis entsprach dem mit uns abgestimmten Verfahren und ergab keine Anhaltspunkte für weitere

Prüfungen. Aus diesem Grund gehen wir davon aus, dass auch bei den übrigen relevanten VAwS-Datensätzen die Löschungen bzw. Anonymisierungen in entsprechender Weise vorgenommen worden sind. Die zuständige Aufsichtsbehörde nach dem Wasserrecht haben wir entsprechend unterrichtet.

11. Soziales

11.1 Projekt SAM der Allgemeinen Ortskrankenkassen

Unsere Forderungen zur datenschutzgerechten Entwicklung des Verfahrens werden von den Allgemeinen Ortskrankenkassen ernst genommen.

Im Berichtszeitraum haben wir weiter im Rahmen einer Unterarbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Entwicklung der neuen Software SAM begleitet. Sie hat inzwischen nicht nur den neuen Namen oscare® erhalten, sondern es ist auch gelungen, datenschutzrechtliche Fortschritte zu erzielen (vgl. 19. TB, 6.3). Die Version 1.0 wurde zwischenzeitlich bei fast allen Allgemeinen Ortskrankenkassen produktiv gesetzt. Dabei konnte die Software ihre „Massendatenfähigkeit“ unter Beweis stellen. Die Pilotierung des Sachleistungswesens einschließlich des Bereichs der Krankenhauspflege (oscare® 2.0) soll im Laufe des Jahres 2006 bei der AOK Rheinland-Pfalz erfolgen. Dabei muss aus datenschutzrechtlicher Sicht allerdings an einigen Punkten noch weiter gearbeitet werden. Nachfolgend nur einige Beispiele:

- Die im Sozialgesetzbuch (SGB) vorgesehenen Speicherungsfristen müssen in ein Löschkonzept einfließen. Dies gilt sowohl für den operativen Datenbestand als auch für die Archivierung im Dokumenten-Management-System. Auch das Business-Warehouse, das eine Spiegelung des gesamten operativen Datenbestandes beinhalten soll, muss in das Löschkonzept einbezogen werden.

  Die Projektleitung hat zwar bereits Teile eines Löschkonzeptes vorgelegt. Die Fragen sind aber noch nicht abschließend geklärt, insbesondere noch nicht die Abgrenzung der Verantwortlichkeit des AOK-Bundesverbandes einerseits und der Allgemeinen Ortskrankenkassen auf Landesebene andererseits. Offen ist auch, welche konkreten Löschfristen im Dokumenten-Management-System und im Business-Warehouse definiert werden sollen. Dagegen ist bereits klar, dass innerhalb des Business-Warehouse eine physikalische Löschung von Daten möglich ist. Darüber hinaus ist sicher gestellt, dass Daten, die in den operativen Systemen bereits gelöscht sind, auch im Business-Warehouse nicht mehr zur Verfügung stehen. Die weitere Entwicklung des Löschkonzeptes soll mit uns abgestimmt werden.

- Die Software sieht die Berechnung eines Deckungsbeitrags vor, der zunächst versichertenbezogen gespeichert werden sollte. Wir hatten deshalb die Projektleitung insbesondere um die Darlegung der Rechtsgrundlage für eine versichertenbezogene Speicherung des Deckungsbeitrags gebeten und betont, dass dem Betroffenen insoweit ein Auskunftsanspruch zusteht. Die Projektleitung hat daraufhin ein neues Konzept entwickelt. Eine versichertenbezogene Speicherung des Deckungsbeitrags als Datenfeld ist nicht mehr vorgesehen. Im Business-Warehouse sind zwar alle Daten, aus denen sich der Deckungsbeitrag zusammensetzt, ständig gespeichert und sie werden dort auch aktualisiert. Bestimmte Mitarbeiter sollen berechtigt sein, aktuelle Auswertungen der Deckungsbeiträge ausrechnen zu lassen. Die Auswertungen sollen aber keine Deckungsbeiträge für einzelne Versicherte enthalten, sondern lediglich aggregierte Darstellungen. Deckungsbeiträge für einzelne Versicherte spielen daher nur im Rahmen dieser Berechnungen eine Rolle. Das Zugriffskonzept soll entsprechende Restriktionen enthalten. Der AOK-Bundesverband wird den Allgemeinen Ortskrankenkassen auf Landesebene mitteilen, dass die Standardeinstellungen zur Deckungsbeitragsberechnung nicht verändert werden dürfen.

  Durchgreifende datenschutzrechtliche Bedenken bestehen damit nicht mehr. Wir halten es aber für erforderlich, durch technische und organisatorische Maßnahmen zu unterbinden, dass im Zeitpunkt der Erzeugung von Deckungsbeiträgen auf individuelle Werte zugegriffen werden kann. Darüber hinaus sollte der AOK-Bundesverband die Allgemeinen Ortskrankenkassen auf Landesebene vorsorglich schriftlich darüber informieren, dass Deckungsbeiträge nicht personenbezogen gespeichert werden sollen. Dies wurde uns von der Projektleitung zugesichert. Endgültig werden unsere Bedenken allerdings erst ausgeräumt sein, wenn uns weitere Erläuterungen zum technischen Prozess der Berechnung von Deckungsbeiträgen vorliegen. Die entsprechenden Unterlagen sollen wir von der Projektleitung im Jahr 2006 erhalten.

- Im Zusammenhang mit dem von uns immer wieder bemängelten, aber nach wie vor vorgesehenen geschäftsstellenübergreifenden Zugriff auf Versichertendaten hatten wir verlangt, dass die tatsächlichen Zugriffe der einzelnen Nutzer für einen begrenzten Zeitraum zu protokollieren sind. Da die Software dies bislang nicht leisten kann, haben wir die Projektleitung auf Referenzobjekte für die Entwicklung eines solchen Protokollverfahrens hingewiesen. Da grundsätzliche technische Probleme der von uns geforderten Protokollierung nicht entgegen stehen, kann auf deren Realisierung nicht verzichtet werden. Die Projektleitung prüft unsere Hinweise.

Die vollständige Ablösung des Altsystems IDVS II wird nach den derzeitigen Planungen wohl erst im Jahr 2010 erfolgen können. Bereits jetzt ist aber

erkennbar, dass die Entwicklung von oscare® im Bereich der gesetzlichen Krankenversicherung mit großem Interesse verfolgt wird. Als erste Krankenkasse, die nicht zur AOK-Organisation gehört, wird die Barmer Ersatzkasse im Laufe des Jahres 2006 mit dem Einsatz vorn oscare® beginnen. Es ist also nicht ausgeschlossen, dass sich oscare® zu einer Branchensoftware entwickelt. Deshalb ist es umso wichtiger, dass wir den Prozess weiter aufmerksam verfolgen. Daran ist auch die Projektleitung interessiert.

11.2 Arbeitslosengeld II

Gravierende Datenschutzmängel beim Arbeitslosengeld II müssen endlich beseitigt werden.

Zum Jahresbeginn 2005 trat das Sozialgesetzbuch Teil II (SGB II) in Kraft. Durch die Zusammenlegung von Arbeitslosenhilfe und Sozialhilfe entstand das neue Arbeitslosengeld II. Die Aufgabe wird in Hamburg wahrgenommen durch die team.arbeit.hamburg (Hamburger Arbeitsgemeinschaft SGB II – ARGE). Die Frage, ob die Zuständigkeit des Hamburgischen Datenschutzbeauftragten für die Arbeitsgemeinschaft SGB II gegeben ist, hat die Behörde für Wirtschaft und Arbeit (BWA) eindeutig bejaht. Danach sind wir gemäß § 81 SGB X ausschließlich zuständig, da die ARGE als öffentliche Stelle des Landes tätig ist.

Bei der Umsetzung der Zusammenlegung von Arbeitslosenhilfe und Sozialhilfe hat es erhebliche datenschutzrechtliche Mängel gegeben, durch die die Rechte der Betroffenen stärk beeinträchtigt werden. Dies lag überwiegend nicht an Missständen in Hamburg, sondern an unzureichenden Vorgaben von Seiten der Bundesagentur für Arbeit (BA) in Nürnberg. So wurden die Antragsformulare von Beginn an von uns kritisiert, weil sie viele Fragen enthielten, die aus datenschutzrechtlicher Sicht nicht gestellt werden durften. Da es sich um Vordrucke handelt, die bundeseinheitlich von der BA vorgegeben werden, haben wir gemeinsam mit den anderen Landesdatenschutzbeauftragten und dem Bundesbeauftragten für den Datenschutz auf Korrekturen gedrängt. Nicht ohne Erfolg, denn die BA hat zwischenzeitlich den Antragsvordruck und die Zusatzblätter überarbeitet. Verabredet war aber, dass die Betroffenen ergänzende Ausfüllhinweise erhalten, um ihnen ein datenschutzgerechtes Ausfüllen der Unterlagen zu ermöglichen. Insbesondere soll damit eine Erhebung von nicht erforderlichen Daten vermieden werden. Leider müssen wir feststellen, dass die Ausfüllhinweise nicht allen ARGE-Mitarbeitern bekannt sind. Die ARGE ist deshalb von uns aufgefordert worden, geeignete Maßnahmen zu treffen, damit allen Betroffenen nicht nur baldmöglichst die neuen Antragsvordrucke, sondern diese gemeinsam mit den Ausfüllhinweisen ausgehändigt werden.

Erhebliche datenschutzrechtliche Bedenken bestehen auch gegen die von der BA entwickelte Datenverarbeitungssoftware A2LL, die von der ARGE zur Berechnung der Leistungen eingesetzt werden muss. So mangelt es an einem Zugriffsberechtigungskonzept und einer Protokollierung der Zugriffe. Damit ist es den über 40.000 Beschäftigten in der BA und in den Arbeitsgemeinschaften nach SGB II möglich, voraussetzungslos auf die Daten aller Leistungsempfänger zuzugreifen, ohne dass eine Kontrolle möglich wäre. Diese Mängel wurden durch den Bundesbeauftragten für den Datenschutz bereits beanstandet. Eine Abhilfe war bis zum Redaktionsschluss jedoch nicht erkennbar, obwohl sowohl das Bundesministerium für Wirtschaft und Arbeit (BMWA) als auch die BA zugesagt hatten, die datenschutzrechtlichen Defizite im Laufe des Jahres 2005 zu beheben.

Dies gilt auch für das elektronische Vermittlungsverfahren coArb, das ebenfalls allen Mitarbeitern einen bundesweiten lesenden Zugriff erlaubt. Äußerst sensible Daten, wie z. B. Vermerke über Schulden-, Ehe- oder Suchtprobleme, können so eingesehen werden. Den Datenschutzbeauftragten sind bereits Missbrauchsfälle bekannt geworden. Einzelne Arbeitsgemeinschaften reagieren auf die Probleme und speichern ihre Unterlagen wieder in Papierform. Es muss sichergestellt sein, dass das Nachfolgesystem VerBIS, das Mitte 2006 einsatzbereit sein soll, grundsätzlich nur noch einen engen, regionalen Zugriff zulässt und ein detailliertes Berechtigungs- und Löschungskonzept beinhaltet. Der Datenschutz muss auch bei der Migration der Daten aus coArb in VerBIS gewährleistet sein.

Auf der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 in Lübeck wurde wegen der gravierenden Mängel beim Arbeitslosengeld II eine Entschließung gefasst, in der die BA und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene aufgefordert werden, selbst und im Rahmen ihrer Rechtsaufsicht die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Zu der notwendigen völligen Neugestaltung des Systems A2LL wegen der offenbar nicht zu beseitigenden Defizite erwarten die Datenschutzbeauftragten ihre zeitnahe Beteiligung. Es ist sicherzustellen, dass die datenschutzrechtlichen Vorgaben, wie die Protokollierung der lesenden Zugriffe und ein klar definiertes Zugriffsberechtigungs- und Löschungskonzept, ausreichend berücksichtigt werden, um den Schutz des informationellen Selbstbestimmungsrechts der Antragsteller zu gewährleisten. Wir haben diese Entschließung sowohl der hamburgischen ARGE als auch der BWA zur Kenntnis gebracht und damit die Forderung verbunden, bei der Behebung der datenschutzrechtlichen Defizite im Rahmen ihrer Möglichkeiten mitzuwirken.

Bei aller Kritik ist zu sagen, dass sowohl die hamburgische ARGE als auch die BWA bislang aufgeschlossen auf unsere Hinweise reagiert haben. So konnten

wir insbesondere erreichen, dass die Steuerung und Bedienung der Kunden in den Jobcentern unter datenschutzrechtlichen Gesichtspunkten verbessert wurde. Das bezieht sich beispielsweise auf die Schaffung von Diskretionszonen und das Angebot, auf Wunsch Antragsteller in einem Einzelzimmer zu bedienen. Wir werden in 2006 die Arbeitsabläufe in den Jobcentern noch genauer untersuchen und dabei die Aktenführung, die Verwendung von Einwilligungserklärungen und Schweigepflichtentbindungserklärungen sowie die Realisierung des Anspruchs auf Akteneinsicht nach § 25 SGB X bzw. auf Auskunft nach § 83 SGB X prüfen.

11.3 Projekt Informierte Jugendhilfe (InfoJu)

Der Datenschutz steht einem optimierten Informationsfluss in der Jugendhilfe nicht entgegen, wenn es um Maßnahmen zur Verbesserung des Schutzes von Kindern geht.

Der tragische Tod der 7-jährigen Jessica im Frühjahr 2005 hat Hamburg erschüttert. Die zuständigen Stellen waren deshalb aufgerufen, alles zu tun, um die Wiederholung eines solchen Falles extremer Kindesvernachlässigung strukturell zu verhindern. Dazu sind sie auf Informationen und Daten auch aus anderen Verwaltungsbereichen, aus Nachbarschaft sowie von gesellschaftlichen Institutionen angewiesen. Da im Fall Jessica die Informationsmöglichkeiten offensichtlich nicht ausgeschöpft wurden, hat der Senat eine Projektgruppe „Informierte Jugendhilfe“ eingesetzt, die Verbesserungen für die Informationsflüsse zu den Jugendämtern entwickeln soll. An der Projektarbeit sind wir von Beginn an beteiligt worden. Aus datenschutzrechtlicher Sicht sind dabei zahlreiche Punkte angesprochen worden, von denen folgende besonders wichtig sind:

1. Die Jugendämter sahen es als geboten an, die Aufbewahrungsfristen für Akten des Jugendamtes in folgenden Fällen zu verlängern:
   - Kindestodesfälle in einer Familie bei begründetem Verdacht im Allgemeinen Sozialen Dienst (ASD) auf vorangegangene Kindeswohlgefährdung.
   - Kindeswohlgefährdung durch sexuelle Übergriffe, körperliche Misshandlungen und Vernachlässigungen, bei denen eine Meldung nach § 50 Abs. 3 SGB VIII durch den ASD an das Familiengericht erfolgt ist.
   - Psychische Erkrankungen und Suchtkrankheiten (jeweils verifiziert durch psychiatrische Behandlungen) von Müttern, Vätern oder Jugendlichen (die später selber Eltern werden können).
   - Jugendliche, die wegen erlebter Kindeswohlgefährdung untergebracht wurden und als werdende Mutter bzw. werdender Vater aus stationärer Jugendhilfe entlassen werden.

Wir haben einer Verlängerung der Aufbewahrungsfrist von fünf auf zehn Jahre zugestimmt. Bei den in Rede stehenden Fällen, die aus jugendamtlicher Sicht für eine Verlängerung der Aufbewahrungsfrist von Akten sprechen, handelt es sich um spezielle Problemkonstellationen. Es ist nicht von der Hand zu weisen, dass in solchen Fällen die Akte zu einem späteren Zeitpunkt für eine ordnungsgemäße Aufgabenerfüllung des Jugendamtes wieder benötigt werden kann. Die Notwendigkeit der gegenüber dem „Normalfall" verlängerten Aufbewahrung muss dargetan und die ansonsten ordnungsgemäße Behandlung der Akten sicher gestellt werden. Dies erfordert, dass

- angegeben wird (z. B. in einem Formblatt), in welche der genannten vier Fallkategorien der verlängerten Aufbewahrung die Akte einzuordnen ist,
- die – verlängerte – Aufbewahrungsfrist für die Akte kenntlich gemacht wird,
- die Rechte des Betroffenen auf Auskunft, Berichtigung oder Löschung nach § 84 SGB X unberührt bleiben.

2. Es wurde an uns die Frage herangetragen, inwieweit Rückmeldungen des Jugendamtes an den Informationsgeber einer (vermeintlichen) Kindeswohlgefährdung zulässig sind. Insbesondere stellte sich die Frage, ob die Nennung des für den Fall zuständigen Sachbearbeiters beim ASD und des Aktenzeichens an die die Information gebende öffentliche Stelle zulässig ist. Wir sind dabei zu dem Ergebnis gekommen, dass die Nennung des zuständigen Sachbearbeiters und des Aktenzeichens, unter dem der Information nachgegangen wird, datenschutzrechtlich unproblematisch sind. Eine Übermittlung von Daten über die vom Jugendamt gewonnenen Erkenntnisse oder ergriffenen Maßnahmen kommt nicht in Betracht.
3. In einem bei der Behörde für Bildung und Sport (BBS) geführten zentralen Schülerregister sollen ab dem Schuljahresbeginn 2006 / 2007 alle schulpflichtigen Kinder und alle Kinder, die eine Schule in Hamburg besuchen, erfasst werden. Andere Behörden sollen Auskünfte erhalten oder online Einsicht in das Register nehmen können. Der Senat wird der Bürgerschaft im Frühjahr 2006 den Entwurf einer entsprechenden gesetzlichen Ermächtigung zur Beschlussfassung und den Entwurf einer Rechtsverordnung zur Kenntnisnahme vorlegen, aus dem die Einzelheiten über die im Register gespeicherten Daten sowie Anlass und Umfang ihrer Verarbeitung hervorgehen. An den gesetzgeberischen und technischen Vorbereitungen zur Umsetzung, die bereits aufgenommen wurden, sind wir beteiligt.
4. Kindertageseinrichtungen stehen in regelmäßigem und engem Kontakt mit Kindern und Familien. Gefährdungssituationen, die sie erkennen, aber durch eigene Aktivitäten nicht beheben können, melden sie bereits jetzt an die Jugendämter. Die Kindertagesstätten sollen zukünftig einen unter unse-

rer Mitwirkung entwickelten Handlungsleitfaden zum Erkennen von Kindeswohlgefährdungen anwenden. Die Zusammenarbeit wird künftig durch die Einführung von mit uns abgestimmten Formularen vereinfacht werden.

5. Anzeichen von Kindeswohlgefährdungen können besonders häufig im Schulalltag auftreten. Neben Lernschwierigkeiten spielen soziale und familiäre Probleme und auch Schulpflichtverletzungen eine Rolle. Zur Abwendung von Gefährdungen werden die Lehrkräfte von den Regionalen Beratungs- und Unterstützungsstellen (REBUS) unterstützt. Soweit in diesem Zusammenhang Maßnahmen erforderlich werden, die über den Erziehungsauftrag und die Kompetenzen der Schule hinausgehen, müssen sie mit anderen Stellen koordiniert werden, u. a. den Jugendämtern. Zur Verbesserung der praktischen Arbeit haben die Behörde für Soziales und Familie und die Behörde für Bildung und Sport unter Beteiligung der Jugendämter zwei Arbeitsgruppen eingerichtet. Sie sollen Handlungsempfehlungen zu typischen Fällen erarbeiten, die eine geregelte Zusammenarbeit zwischen Jugendämtern, Schulen und REBUS erfordern.

   Wir haben gebeten, uns auch an diesen Arbeitsgruppen zu beteiligen. Bei der Gelegenheit möchten wir die in der Vergangenheit von uns bei REBUS festgestellten datenschutzrechtlichen Defizite (vgl. 19. TB, 10.1) aufarbeiten. Deshalb haben wir zunächst darauf verzichtet, die von uns begonnene Querschnittsprüfung von REBUS fortzusetzen.

6. Für Ärzte und Angehörige anderer Heilberufe sollen mögliche Hindernisse beseitigt werden, Kindeswohlgefährdungen, die ihnen bekannt werden, an Jugendämter mitzuteilen. Der Senat will daher auf Verdeutlichungen der Offenbarungsbefugnisse in den Berufsordnungen hinwirken. Die Behörde für Wissenschaft und Gesundheit soll der Ärztekammer einen entsprechenden, mit uns abgestimmten Formulierungsvorschlag zur Ergänzung der Berufsordnung der Hamburger Ärzte unterbreiten. Diese Regelung würde bedeuten, dass der Schutz von Kindern vor Misshandlung, Missbrauch und schwerwiegender Vernachlässigung den Arzt bei jedem ernsthaften und begründeten Verdacht zu einer Informationsweitergabe an die Jugendämter befugt. Für die Angehörigen anderer Heilberufe, die wie die Ärzte gemäß § 203 Absatz 1, Nummer 1 StGB der Schweigepflicht unterliegen, soll auf eine analoge Regelung hingewirkt werden.

7. Zur Verbesserung des Informationsaustausches zwischen Polizei und Jugendämtern sollen die Jugendämter der Polizei regelhaft eine Rückmeldung geben, aus der die bearbeitende Stelle des Jugendamtes hervorgeht. Die Meldungen sollen nach dem Vorbild des Rückmeldesystems, das bei der Zusammenarbeit zwischen dem Familieninterventionsteams (FIT) und der Polizei unter unserer Mitwirkung bereits erprobt wurde, möglichst elektronisch erfolgen. Solche Rückmeldungen erleichtern die spätere Kon-

taktaufnahme zwischen den betreffenden Mitarbeitern des Jugendamtes und der Polizei. Datenschutzrechtliche Bedenken bestehen dagegen nicht.

8. Für die Jugendämter ist ein datenschutzgerechtes Formblatt entwickelt worden, mit dem sie bei einer zentralen Ansprechstelle der Staatsanwaltschaft gezielt abfragen können, ob bestimmte Personen kindeswohlrelevante Straftaten begangen haben. Darüber hinaus will der Senat eine Bundesratsinitiative ergreifen, die den Jugendämtern einen Online-Zugriff auf das Bundeszentralregister ermöglicht. Der Online-Zugriff soll auf „rechtskräftige Verurteilungen wegen kindeswohlgefährdender Straftaten" beschränkt sein. Eine derartige sektorale Beschränkung des Zugriffs auf einzelne, relativ vage umschriebene Straftaten ist im Bundeszentralregistergesetz (BZRG) jedoch nicht vorgesehen und in der Praxis nicht realisierbar. Der Senat will dabei unterscheiden zwischen „besonders gefährdungsrelevanten Straftaten" und „tendenziell gefährdungsrelevanten Straftaten". Die letztgenannte Kategorie von Straftaten zeichnet sich dadurch aus, dass sich die Gefährdung des Kindeswohls erst auf Grund einer individuellen Prüfung erschließt. Wie diese Prüfung im Falle eines Online-Zugriffs vorab geleistet werden soll, zumal bei einem Register, das zu den Beweggründen des Täters, der Ausführung und den Auswirkungen der Tat oder anderen gefährdungsrelevanten Umständen keine Angaben enthält, ist völlig unklar. Erst eine Auswertung der Strafverfahrensakten nach bereits erfolgtem Online-Abruf aus dem Bundeszentralregister könnte zeigen, ob das Jugendamt mit seiner Einschätzung der Kindeswohlgefährdung richtig lag oder nicht.

   Wir sind an der Abstimmung der angekündigten Bundesratsinitiative zur Änderung des BZRG zu beteiligen und werden eine sorgfältige Prüfung vornehmen.

9. Es ist vorgesehen, in einem Jugendamt zu erproben, ob die regelmäßige Mitteilung des Einwohneramts über Geburten und Zuzüge von Kindern einen zusätzlichen Nutzen für das frühzeitige Erkennen von Kindeswohlgefährdungen erbringt. Wenn das der Fall ist, soll die Maßnahme flächendeckend umgesetzt werden. Wir haben dem Senat mitgeteilt, dass derartige Datenübermittlungen nach der gegenwärtigen Rechtslage unzulässig sind. Um das Verfahren rechtssicher zu gestalten, bedarf es entsprechender Änderungen in den landesmelderechtlichen Bestimmungen. Wir werden die dafür eingesetzte Arbeitsgruppe entsprechend beraten.

11.4 JobCard-Verfahren

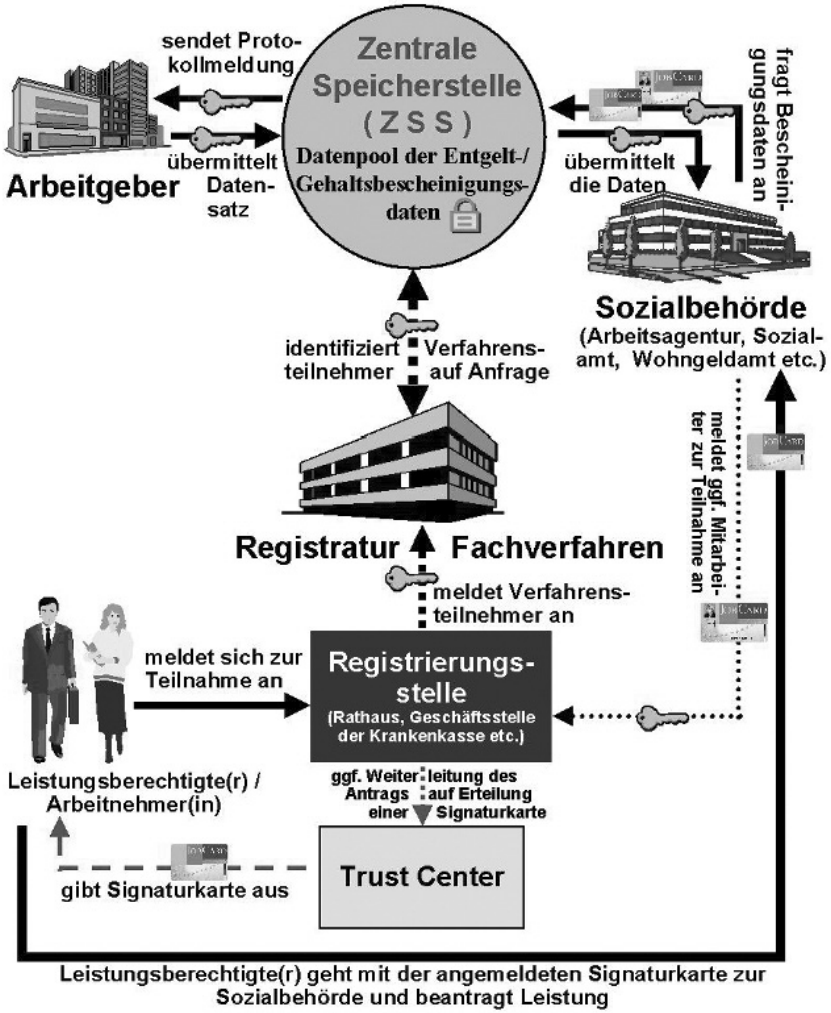
Die verfassungsrechtliche Zulässigkeit ist noch nicht abschließend geklärt. Bei einem zulässigen Verfahren könnte durch die Ver- und Entschlüsselung durch eine unabhängige Stelle die Datensicherheit entscheidend erhöht werden.

Ziel des bundesweiten JobCard-Verfahrens ist es, die Arbeitgeber von der Ausstellung von Entgeltbescheinigungen zu entlasten. Bei zahlreichen Anträgen auf Sozialleistungen (z. B. Arbeitslosengeld II, Wohngeld, Erziehungsgeld) müssen die Antragsteller derzeit ihre Entgeltbescheinigungen in Papierform vorlegen. Dies sind etwa 60 Millionen Bescheinigungen jährlich. Dieser Prozess soll automatisiert und ohne Medienbruch realisiert werden. Dazu soll ein zentraler Entgeltdatenbestand aller Beschäftigten in Deutschland entstehen. Alle ca. 2,8 Millionen Arbeitgeber vom kleinen Kiosk bis zum Großkonzern sollen verpflichtet werden, monatlich die einzelnen Datensätze für ihre Beschäftigten an das Zentralregister zu übermitteln. Dort sollen die Daten bis zu fünf Jahre gespeichert werden. Im Zuge der Antragsbearbeitung sollen die zuständigen Stellen, wie z. B. die Bundesagentur für Arbeit, die erforderlichen Daten aus dem Datenbestand abrufen. Etwa 40 Millionen Bundesbürger wären von diesem Verfahren betroffen.

Ein großer Teil der Daten der zentralen Speicherstelle würde jedoch niemals genutzt werden, da von der betroffenen Person während der Speicherfrist kein Leistungsantrag gestellt werden wird. Die Größe dieser Gruppe hat Auswirkungen auf die Verhältnismäßigkeit des Verfahrens. Die Anzahl der hiervon Betroffenen kann jedoch nicht fundiert abgeschätzt werden, da bisher die entsprechende Zahlenbasis fehlt. Somit kann auch die Erforderlichkeit der Datenerhebung nicht beurteilt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher die Bundesregierung im Oktober 2005 aufgefordert, die verfassungsrechtliche Zulässigkeit zu prüfen und das Ergebnis offen zu legen.

Auch wenn das Ergebnis der Prüfung eine verfassungsrechtliche Zulässigkeit ergeben sollte, ist das vorgesehene technisch-organisatorische Konzept des JobCard-Verfahrens datenschutzrechtlich hoch problematisch, da die zentrale Sammlung einer sehr großen Menge von sensiblen personenbezogenen Daten in hohem Maße Missbrauchsmöglichkeiten bietet und Begehrlichkeiten zur Folge haben kann. Es ist daher ein Höchstmaß an Datenschutz erforderlich, insbesondere auch bei der technischen Umsetzung von Schutzmaßnahmen. Daher sehen die Datenschutzbeauftragten in der Ver- und Entschlüsselung der Daten durch eine unabhängige Vertrauensstelle eine wichtige zusätzliche datenschutzrechtliche Sicherung im Sinne einer Teilung der Verantwortlichkeiten. Es wäre dann ein Vier-Augen-Prinzip gewährleistet, bei der die zentrale Speicherstelle nur Zugriff auf die verschlüsselten Daten hätte und die unabhängige Vertrauensstelle jeweils nur den angeforderten Datensatz entschlüsseln würde, ohne Zugriff auf den gesamten Datenbestand zu erhalten.

Funktionaler Ablauf des JobCard-Verfahrens



Funktionaler Aufbau (BFD, 20. Tätigkeitsbericht)

12. Bildung

12.1 Reform der Lernmittelbeschaffung

In den Schulen wurde ein neues Verfahren zur Lernmittelbeschaffung eingeführt, obwohl noch zahlreiche datenschutzrechtliche Fragen offen sind.

Seit dem Schuljahr 2005 / 06 werden die Lernmittel den Schülern nicht mehr kostenlos zur Verfügung gestellt, sondern müssen von den Eltern sowie den volljährigen Schülerinnen und Schülern selbst beschafft werden. Die Bücher und weitere Lernmittel müssen entweder gekauft oder von der Schule für das Schuljahr gegen Gebühr entliehen werden. Hierfür haben die Schulen von der Behörde für Bildung und Sport (BBS) ein elektronisches Bibliotheksprogramm erhalten, das alle Vorgänge umfassen soll, um die Lernmittelbeschaffung abwickeln zu können. Mit dem Programm werden personenbezogene Daten verarbeitet. Weder den Einsatz noch die Funktionalitäten des Bibliotheksprogramms hat die BBS abschließend mit uns abgestimmt. Insbesondere lag uns bis zum Redaktionsschluss nicht der Anforderungskatalog für die Software vor, den uns die BBS bereits im Dezember 2004 zugesagt hatte.

Kurz vor Beginn des Schuljahres 2005 / 06 wurde uns von der BBS zudem völlig überraschend mitgeteilt, dass der Einsatz des Bibliotheksprogramms und die damit verbundenen Verfahrensabläufe von der BBS nicht verbindlich für alle Schulen einheitlich vorgegeben werden. Den Schulen werde vielmehr die Entscheidung überlassen, ob dieses Produkt überhaupt eingesetzt werden soll und – falls sie sich dafür entscheiden – wie mit dem Produkt das Verfahren abgewickelt werden soll. An einigen Schulen werde mit einem anderen Programm gearbeitet, einige Schulen würden wohl ganz auf die Automatisierung der Abläufe verzichten.

Nach diesem Sachstand baten wir die BBS um Klärung, inwieweit die Projektvorgaben hinsichtlich des Softwareeinsatzes für die Schulen verbindlich sind. Darauf haben wir keine Antwort erhalten. Außerdem muss die BBS entscheiden, ob jede einzelne Schule als Daten verarbeitende Stelle im Sinne von § 4 Abs. 3 Hamburgisches Datenschutzgesetz (HmbDSG) bei der Lernmittelbeschaffung anzusehen ist. Auch hierzu hat sich die BBS nicht geäußert. Sollte die Schule als Daten verarbeitende Stelle gelten, ist es unumgänglich, dass uns jede Schule sowohl eine Risikoanalyse nach § 8 Abs. 4 HmbDSG als auch eine Verfahrensbeschreibung nach § 9 HmbDSG vorlegt. Beide Unterlagen sind vor der Inbetriebnahme des Verfahrens zu erstellen. Bis zum Redaktionsschluss lag uns lediglich eine Risikoanalyse vor, die zentral von der BBS erarbeitet wurde. Eine Verfahrensbeschreibung im Sinne von § 9 HmbDSG haben wir überhaupt nicht erhalten, sondern uns liegt lediglich eine Beschreibung des Herstellers des Bibliotheksprogramms vor, aus der ersichtlich ist, was das Produkt leistet und wie mit den Funktionalitäten umzugehen ist.

Datenschutzrechtliche Fragen treten auch dadurch auf, dass mehrere Personengruppen die Lernmittel weiterhin kostenlos erhalten sollen, sofern sie eine entsprechende Förderberechtigung nachweisen können. Dabei handelt es sich im Wesentlichen um sozial schwächer gestellte Personen, die zum Beispiel Arbeitslosengeld, Hilfen zum Lebensunterhalt und andere bedarfsabhängige Sozialleistungen erhalten. Zudem gibt es eine Ermäßigung der Gebühren für Familien mit drei oder mehr schulpflichtigen Kindern. In diesen Fällen müssen die Erziehungsberechtigten bzw. die Schüler nachweisen, dass sie die Voraussetzungen für die Genehmigung von Vergünstigungen erfüllen. Dazu müssen sie der Schule den entsprechenden Leistungsbescheid oder eine Bescheinigung des Leistungsträgers (also zum Beispiel der Hamburger Arbeitsgemeinschaft SGB II) vorlegen. Bei dieser Förderberechtigung handelt es sich um ein Sozialdatum, das wegen seiner Sensibilität besonders geschützt werden muss. Die hierfür erforderlichen Maßnahmen wurden nicht getroffen. So mangelt es beispielsweise an einer Verschlüsselung der Daten auf den Rechnern.

Des Weiteren konnte bisher nicht geklärt werden, welche Daten in der Protokolldatei des Bibliotheksprogramms wie lange und aus welchem Grund gespeichert werden. Ebenfalls ist unklar, unter welchen Voraussetzungen diese Daten von welchem Personenkreis ausgewertet werden müssen bzw. dürfen.

Überdies haben wir lediglich am Rande erfahren, dass die Reform der Lernmittelfreiheit auch in den beruflichen Schulen umgesetzt werden soll, unsere förmliche Beteiligung ist bislang jedoch nicht erfolgt. Die BBS hatte auf unser Drängen zwar zugesagt, die Verantwortlichen aufzufordern, dies nachzuholen. Dennoch ist dies bis zum Redaktionsschluss unterblieben.

Wegen der datenschutzrechtlichen Unsicherheiten haben wir wiederholt darauf gedrängt, dass die BBS den Schulen aussagekräftige Handreichungen für die Umsetzung der Reform der Lernmittelbeschaffung insgesamt, insbesondere aber zur äußeren Datensicherung aushändigen muss. Nur so kann erreicht werden, dass in den Schulen ein zumindest einigermaßen einheitlicher Datenschutzstandard hergestellt wird. Nach unseren letzten Informationen soll dies erst zu Beginn des zweiten Schulhalbjahres erfolgen. Dies ist aus unserer Sicht nicht hinnehmbar, weil die nach § 8 HmbDSG erforderlichen technischen und organisatorischen Maßnahmen getroffen werden müssen, sobald mit der automatisierten Verarbeitung personenbezogener Daten begonnen wird. Zu den organisatorischen Maßnahmen gehören unabdingbar aussagekräftige Handreichungen für die Mitarbeiter.

Nach alledem hat die BBS die Reform der Lernmittelbeschaffung umgesetzt, ohne vorher dafür zu sorgen, dass den Anforderungen des Datenschutzes entsprochen wird. Hinzu kommt, dass wir von der BBS entweder sehr schleppend oder gar nicht mit den erforderlichen Informationen versorgt worden sind. Wir

werden deshalb weiter darauf drängen, dass die noch vorhandenen datenschutzrechtlichen Defizite behoben werden.

12.2 Videoüberwachung in Schulen

Der zunehmende Einsatz von Videoüberwachungsanlagen in Schulen darf nicht dazu führen, dass die Persönlichkeitsrechte der Schülerinnen und Schüler sowie der Lehrkräfte verletzt werden.

Zahlreiche Schulen gehen seit geraumer Zeit dazu über, Videoüberwachungsanlagen zu installieren. In aller Regel soll damit der Schutz gegen strafbare Handlungen, insbesondere Diebstähle und Sachbeschädigungen, verbessert werden. Die datenschutzrechtlichen Bestimmungen, die für den Einsatz einer Videoüberwachungsanlage beachtet werden müssen, sind den Schulen häufig nicht geläufig.

Die Videoüberwachung ist nur zulässig, wenn sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der Betroffenen bestehen. Dabei reicht allein das Motiv einer allgemeinen abstrakten Gefahrenvorsorge für den Schutz des Eigentums nicht aus. Vielmehr müssen belegbare Tatsachen die Annahme rechtfertigen, dass schwerwiegende Beeinträchtigungen des Eigentums drohen oder die Begehung sonstiger strafbarer Handlungen droht und es diese abzuwehren gilt.

Bei der Konzeption des Einsatzes von Videoüberwachungsmaßnahmen ist als gesetzliche Voraussetzung insbesondere die Erforderlichkeit zu prüfen. Sie ist nur dann gegeben, wenn der beabsichtigte Zweck nicht mit einem anderen zumutbaren Mittel, das weniger in die Rechte der Betroffenen eingreift, erreicht werden kann. Dabei ist auch zu prüfen, ob statt einer umfassenden Einführung der Überwachungstechnik ein Einsatz an Schwerpunkten oder zu bestimmten Zeiten ausreichend ist. Unter dem Gesichtspunkt der Datenvermeidung und Datensparsamkeit ist weiterhin zu prüfen, ob durch den Einsatz spezieller, inzwischen verfügbarer Technik bestimmte Bereiche des Aufnahmefeldes ausgeblendet oder die Gesichter der sich in diesen Bereichen aufhaltenden Personen „verschleiert“ werden können.

In keinem Fall darf die Videoüberwachung an Schulen an die Stelle pädagogischer Maßnahmen oder der Aufsichtspflicht der Lehrer treten, d.h. keine Videoüberwachung von Unterricht und laufendem Schulbetrieb. Unabdingbar ist auch, dass vor der Realisierung einer Videoüberwachung alle Schulgremien damit befasst werden und eine Unterrichtung aller Betroffenen – also insbesondere der Lehrer und Schüler – erfolgt.

Die Zwecke der Videoüberwachung sind vor der Inbetriebnahme der Überwachungsanlage schriftlich zu dokumentieren. Diese Festlegungen sind

sorgfältig vorzunehmen, da die mittels Videoüberwachung gewonnenen Erkenntnisse für andere als die festgelegten Zwecke nicht verwendet werden dürfen. Auch die konkrete Ausgestaltung der Videoüberwachungsanlage hat sich an den festgelegten Zwecken zu orientieren.

In den Fällen, in denen die Videobilder aufgezeichnet werden sollen, ist die Erforderlichkeit auch dafür zu prüfen und auch eine erneute Abwägung der schutzwürdigen Interessen der Betroffenen vorzunehmen. Ferner ist die beabsichtigte Weiterverarbeitung zu dokumentieren. Die Übermittlung der gewonnenen Aufnahmen an Strafverfolgungsbehörden beziehungsweise deren Nutzung als Beweismittel zur Erlangung von Schadensersatz kann zum Erreichen eines dokumentierten Zwecks erforderlich sein. Für einen anderen als den dokumentierten Zweck dürfen die aufgezeichneten Videoaufnahmen nur benutzt werden, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

Sofern Videokameras installiert werden, ist durch Hinweisschilder sowohl auf die Tatsache der Videobeobachtung als auch auf die dafür verantwortliche Stelle hinzuweisen. In der Praxis haben sich hierfür Piktogramme bewährt. Der Hinweis ist deutlich sichtbar anzubringen. Die optische Gestaltung und räumliche Anordnung des Hinweises ist so vorzunehmen, dass sich der Hinweis vor dem Eintritt in den überwachten Bereich im normalen Blickwinkel befindet – also ohne Weiteres wahrnehmbar ist – und nicht erst gesucht werden muss.

Das durch die Videobeobachtung gewonnene Bildmaterial darf nur so lange gespeichert werden, wie es zur Erreichung des verfolgten Zweckes erforderlich ist. Aber auch die Aufnahmen, die für den Beobachtungszweck noch benötigt werden, etwa weil aufklärungsbedürftige Vorkommnisse aufgezeichnet wurden, dürfen nur gespeichert bleiben, wenn schutzwürdige Interessen des Betroffenen nicht entgegenstehen. Die verantwortliche Stelle hat daher die angefallenen Aufnahmen unverzüglich einer Bedarfsprüfung zu unterziehen. In den Fällen, in denen die Aufnahmen nicht mehr für die Erreichung des dokumentierten Aufnahmezwecks benötigt werden, sind diese unverzüglich, d.h. in der Regel innerhalb von ein bis zwei Arbeitstagen, zu löschen. Bei der Konzeption von Überwachungsmaßnahmen sind die hierzu erforderlichen technischen und organisatorischen Maßnahmen vorzusehen.

Diese Rahmenbedingungen für den Einsatz von Videoüberwachungsanlagen in Schulen zeigen, dass zunächst zahlreiche Fragen zu beantworten sind, bevor es zur Installation kommen kann. Die Behörde für Bildung und Sport (BBS) hat auf unser Drängen zugesagt, den Schulen zum Schuljahr 2006 / 2007 Rahmenvorgaben für den Einsatz von Videokameras an die Hand zu geben. Wir haben angeregt, uns bei der inhaltlichen Gestaltung der Handreichung zu beteiligen. Nach unserer Kenntnis verhandelt die BBS mit den pädagogischen Personalräten eine Dienstvereinbarung, die auch das grund-

sätzliche Verfahren zur Entscheidung über den Einsatz einer Videoüberwachungsanlage regelt.

12.3 Videoüberwachung an Hochschulen

Die Universität Hamburg hat gezeigt, dass der Einsatz von Videoüberwachungsanlagen datenschutzgerecht gestaltet werden kann.

Die Universität Hamburg hielt es für erforderlich, verschiedene Bereiche mit einer Videoüberwachungsanlage auszustatten. Einbezogen werden sollten beispielsweise Hörsäle, Bibliotheken und Computer-Pool-Nutzungsräume. Grund für die Maßnahme waren vorwiegend Vandalismusschäden und Diebstähle, die sprunghaft angestiegen waren. Es waren aber nicht nur Sachschäden entstanden, sondern zunehmend waren auch Forschungsergebnisse betroffen, die teilweise nicht mehr ersetzt werden konnten. Wir sind frühzeitig an den Planungen beteiligt worden.

Auf Grund unserer Hinweise ist es gelungen, eine Dienstvereinbarung über den Betrieb von Videoüberwachungsanlagen zu entwickeln, die zwischen der Universität Hamburg und den zuständigen Personalräten geschlossen wurde. Die datenschutzrechtlichen Anforderungen an eine Videoüberwachung wurden dabei in vollem Umfang berücksichtigt. Der Text findet sich im Internet unter www.verwaltung.uni-hamburg.de / k / 7 / hochschulrecht / video_dv.html.

Besonders wichtig war uns, dass ein förmliches und gleichartiges Verfahren eingeführt wird, bevor es zur Installation und Betriebsaufnahme von Videoüberwachungsanlagen kommt. Hierbei handelt es sich um ein Genehmigungsverfahren, das beim Kanzler der Universität Hamburg angesiedelt ist. Dadurch wird ein „Wildwuchs“ in den verschiedenen Bereichen vermieden. In dem Verfahren ist es überdies zwingend, dass dem Kanzler von der beantragenden Einrichtung eine detaillierte Gefährdungsanalyse nach einem definierten Muster vorgelegt wird. Zusätzlich hat das Regionale Rechenzentrum der Universität Hamburg technische Hinweise zur Installation von Videoüberwachungsanlagen entwickelt, die im Rahmen der Dienstvereinbarung verbindlich sind.

Einige der Videoüberwachungsanlagen, die nach dem Inkrafttreten der Dienstvereinbarung in Betrieb genommen wurden, haben wir geprüft. Grundsätzliche datenschutzrechtliche Defizite wurden dabei nicht festgestellt.

13. Gesundheit

13.1 Meldungen zum Krebsregister

Die Prüfung der Krebsregister-Meldungen in der LBK Hamburg GmbH gab Anlass, das Verfahren neu zu regeln, um der Dokumentationspflicht zu genügen.

Auch im Universitätsklinikum Hamburg-Eppendorf – UKE wurde das Verfahren neu und datenschutzgerecht gestaltet.

Nach dem Hamburgischen Krebsregistergesetz sind Ärztinnen und Ärzte berechtigt (nicht verpflichtet), Krebspatienten mit Namen und Krankheitsdaten an das Krebsregister zu melden, wenn der Patient oder die Patientin zuvor eingewilligt hat. Ausnahmsweise darf auf eine Einwilligung verzichtet werden, wenn der Patient verstorben ist oder wenn er (nicht nur vorübergehend) nicht einwilligen kann. Auch wenn der Patient über seine Erkrankung nicht aufgeklärt wurde, um eine ernsthafte Gesundheitsverschlechterung zu vermeiden, darf ohne Einwilligung an das Krebsregister gemeldet werden. Die Meldung mit oder ohne Einwilligung ist nach allgemeinem Medizin- und ärztlichem Berufsrecht in den Behandlungsunterlagen des Patienten zu dokumentieren.

Unsere Prüfung in einem LBK-Krankenhaus 2004 ergab Folgendes: Nach Auskunft des Krebsregisters erfolgten über 66 % der Meldungen ohne Einwilligung, in der Urologie waren es über 82 %. In den Behandlungsakten (Stichproben) des Krankenhauses fand sich keinerlei Hinweis auf die Meldung – weder auf die erforderliche Aufklärung, noch auf die Person des Meldenden, noch auf die erfolgte Einwilligung oder auf einen Ausnahmetatbestand.

Mit der Datenschutzbeauftragten des LBK vereinbarten wir die notwendigen Schritte zur Behebung der Mängel. Ihre Gespräche mit den Ärztlichen Direktoren der LBK-Krankenhäuser führten schließlich zur Vereinbarung eines datenschutzgerechten Verfahrens. In einem Schreiben der LBK-Unternehmensleitung an alle Ärztlichen Direktoren wurde – mit Wirkung vom 1.1. 2005 – Folgendes festgelegt:

- „Ein Einverständnis zur Weitergabe seiner (des Patienten) Daten an das Hamburgische Krebsregister muss eingeholt werden.
- Die Einholung dieses Einverständnisses kann mündlich erfolgen.
- Über die Einholung des Einverständnisses ist eine Notiz in der Krankenakte an einer Stelle niederzulegen, die gut aufgefunden werden kann.
- Wenn einem Patienten die Konfrontation mit seiner Diagnose nicht zugemutet werden kann, weil daraus Schaden resultiert, kann im Ausnahmefall auch auf die Einholung des Einverständnisses verzichtet werden. Dieses ist als Ausnahmetatbestand ebenfalls zu dokumentieren."

Die nur mündliche, aber dokumentierte Einwilligung des Patienten ist ausreichend, weil das Krebsregister keine Schriftlichkeit fordert und das Hamburgische Krankenhausgesetz bestimmt: „Wird die Einwilligung wegen besonderer Umstände (hier: die aktuelle Konfrontation mit einer bösartigen Erkrankung) nur mündlich erteilt, so ist dies aufzuzeichnen." Auch die starke Vereinfachung der gesetzlichen Ausnahmetatbestände im Schreiben der Unternehmensleitung haben wir akzeptiert, um die Bereitschaft der Ärztinnen und Ärzte zu erhalten, das Krebsregister weiterhin durch Meldungen zu unter-

stützen. Im Zusammenhang mit der – ggf. mündlichen – Einwilligung kann allerdings auf eine entsprechende Aufklärung nach dem Krebsregistergesetz nicht verzichtet werden.

Auch bei der Prüfung einer Klinik des Universitätsklinikums Hamburg-Eppendorf (UKE) stießen wir auf ein datenschutzwidriges Verfahren zur Krebsregister-Meldung: Die Einwilligung war in eine allgemeine Einwilligungserklärung zur Nutzung von Gewebe- und Blutproben zu Forschungszwecken integriert. Die Aufklärung über das Krebsregister fehlte ebenso wie die Möglichkeit, die Einwilligung unabhängig von der Forschungsklausel abzulehnen.

Eine neu formulierte eigenständige „Patienteninformation zur Einwilligung in die Meldung an das Hamburgische Krebsregister“ mit schriftlicher Einwilligung half diesem Mangel inzwischen ab. Darüber hinaus haben die Datenschutzbeauftragte des UKE und die Abteilung „Qualitätsmanagement“ des UKE eine übergreifende Verfahrensanweisung erarbeitet, die den Anforderungen des Hamburgischen Krebsregistergesetzes gerecht wird. Sie sieht neben der schriftlichen Aufklärung ein Arzt-Patienten-Gespräch und die Dokumentation der Einwilligung in der Patientenakte und im EDV-System SAP IS-H vor. Abgelehnt hatten wir eine erste Überlegung des UKE, eine „vorsorgliche“ Einwilligungserklärung in den allgemeinen Behandlungsvertrag aufzunehmen. Dies wäre eine überraschende Klausel und würde tatsächlich Betroffene nicht ausreichend und zielgerichtet aufklären. Die Verfahrensanweisung wurde vom Vorstand des UKE Ende Oktober 2005 in Kraft gesetzt.

13.2 Projekt „SEAMAN“: Standardisiertes Aufnahme- und Entlassungsmanagement

Ein einheitliches EDV-Dokument mit Behandlungs- und Pflegedaten von Patienten, auf das Krankenhaus, Ärzte, Pflegedienst und andere Gesundheitsstellen Zugriff haben, bedurfte der datenschutzrechtlichen Modifikation.

Das Projekt „SEAMAN“ („Aufnahme- und Entlassungsmanagement von Krankenhauspatienten im Raum Harburg / Süderelbe“) will das Verfahren optimieren, mit dem Patienten von einer Institution des Gesundheitswesens zu einer anderen wechseln, z. B. aus einem Krankenhaus in die Betreuung durch den Hausarzt und / oder einen Pflegedienst. Alle für eine solche „Überleitung“ relevanten Daten zu Behandlung, Medikation, Befunden, Pflege und psychosozialem Status sollen in vordefinierten Feldern eines einheitlichen elektronischen Dokuments (Überleitungsformular „SEADOK“) gesammelt und allen beteiligten Gesundheitsstellen zur Verfügung gestellt werden. Neben Datenübermittlungen per Fax oder E-Mail ist auch die Zwischenspeicherung des Dokuments auf einem Rechner vorgesehen, auf den die Beteiligten Zugriff erhalten. Die dafür notwendige technische Infrastruktur wird vom „Hamburger Gesundheitsnetz“ auf einem vom Internet abgeschotteten Netz bereitgestellt.

Die Teilnahme des Patienten an diesem Projekt ist freiwillig. Das Krankenhaus oder der Hausarzt – Mitglied bei SEAMAN –, klärt den Patienten mit einem Informationsblatt über das Verfahren auf. In der Einwilligungserklärung benennt der Patient schriftlich die Gruppe von Personen und Stellen, „die mich gemeinsam behandeln und betreuen werden". Dieser Gruppe dürfen nach der Einwilligung „Bilder, Berichte und weitere medizinische Dokumente ... zur Verfügung gestellt werden." Der Patient darf „einem Arzt, Therapeuten o.ä. das Recht entziehen, meine Daten einzusehen" und „jederzeit die Löschung meiner Daten aus dem System beantragen".

Datenschutzrechtlich warf das Projekt eine Reihe von grundsätzlichen Fragen auf. So war zu klären, ob alle in dem einheitlichen Dokument zusammengestellten Daten wirklich für alle Zugriffsberechtigten zur jeweiligen Aufgabenerfüllung erforderlich sind. Warum muss der nur noch zum regelmäßigen Verbandswechsel engagierte Pflegedienst alle vom Krankenhaus eingegebenen Diagnosen und Behandlungsdaten des Patienten erfahren? Reicht nicht die einmalige aktuelle „gerichtete" Datenübermittlung zwischen den Überleitungsbeteiligten (Krankenhaus / Hausarzt / Pflegedienst) aus?

Inzwischen wurde in der Patienteneinwilligung klargestellt, dass der Patient im Zeitpunkt der konkreten Überleitung noch einmal ausdrücklich über die aktuellen Informationsadressaten zu befragen ist und Änderungen in der „Behandlergruppe" dokumentiert werden müssen.

Die Gültigkeit des jeweiligen Überleitungsdokuments (SEADOK) wird nun auf 30 Tage begrenzt. Danach wird es zunächst gesperrt und später gelöscht. Mit der Sperrung ist ein Zugriff auch der an der Überleitung Beteiligten auf das Einheitsdokument im Netz nicht mehr möglich. Bei einer Wiederaufnahme des Patienten in das Krankenhaus wird ein neues Dokument erstellt, wobei die Identitätsdaten aus dem bei der SEAMAN-Anmeldung gespeicherten Stammdatensatz übernommen werden. Auf das alte SEADOK können die Behandler zurückgreifen, wenn sie es – wie regelmäßig – auch in ihrem eigenen EDV-System abgelegt haben.

Es gibt für die Patienten allerdings keine Möglichkeit, einzelnen Ärzten nur bestimmte Daten zugänglich zu machen oder die Teilnahme am Verfahren von vornherein zeitlich zu beschränken – z. B. auf die gerade anstehende Entlassung aus dem Krankenhaus und die Übernahme durch den Hausarzt. Die Vorschriften des Sozialgesetzbuchs zur zukünftigen elektronischen Patientenkarte räumen den Patienten dagegen weitergehende Wahlrechte ein.

Schließlich wurde dem Patienten – nach der zunächst vorgesehenen Information – bei der Einwilligung keineswegs klar, welche konkreten Daten er über SEADOK offenbart bzw. offenbaren wird. Inzwischen wurde in die Einwilligungserklärung eine Übersicht über die Kapitel und die wesentlichen Daten von SEADOK eingefügt, so dass der Patient bereits bei seiner Teilnahme-

entscheidung weiß, auf welchen zu offenbarenden Datenumfang er sich einlässt. Er soll auch einen Ausdruck von SEDAOK erhalten können, um sich selbst und ggf. Ärzte, die nicht an SEAMAN teilnehmen, über diese Daten informieren zu können.

Nach wesentlichen datenschutzrechtlichen Verbesserungen des Verfahrens haben wir gegen eine praktische Pilot-Anwendung von SEAMAN keine Einwände mehr geäußert. Viele Einzelheiten können erst im konkreten Betrieb geklärt werden. Das gilt auch für einige datenschutzrechtliche und datensicherungstechnische Fragen. Zu deren weiterer Klärung bleiben wir mit dem Projektträger im Gespräch.

13.3 Zugriff niedergelassener Ärzte auf Krankenhausdaten

Die LBK Hamburg GmbH und das UKE streben eine engere Kooperation mit niedergelassenen Ärzten an. Der beabsichtigte externe Zugriff auf Patientendaten des Krankenhauses muss datenschutzrechtlichen Rahmenbedingungen genügen, um den Patientenwillen und sein Recht auf freie Arztwahl ausreichend zu berücksichtigen.

Die LBK Hamburg GmbH bereitet ein Pilotprojekt „Einweiserportal“ vor. Ziel ist eine Verkürzung der Krankenhausverweildauer und die Vermeidung von Doppeluntersuchungen durch einen elektronischen Informationsaustausch ohne Medienbrüche. Internet-gestützte Zugriffe auf Krankenhausdaten ihrer Patienten sollen zudem niedergelassene Ärzte stärker an ein LBK-Krankenhaus binden.

Technisch wird der sichere Zugriff aus der Praxis-Software des niedergelassenen Arztes auf die Patientendaten im geschlossenen Krankenhausbereich durch eine Akkreditierung des Arztes bei einem Trust Center, eine persönliche SmartCard (Chip-Karte), die Eingabe einer PIN und durch Verschlüsselungs-Technologien gewährleistet. Ein Problem ist das technische Anforderungsprofil für die anzuschließenden Praxis-EDV-Systeme: Um kein Risiko für das Gesamtsystem einzugehen, müssen die Praxis-Systeme strengen Sicherheitsstandards genügen.

Zur Einbeziehung der Patientinnen und Patienten in das Verfahren schlug die LBK Hamburg GmbH eine Ergänzung der Allgemeinen Geschäftsbedingungen des Behandlungsvertrages um folgenden Satz vor: „Ist Ihr einweisender Arzt mit dem Krankenhaus elektronisch vernetzt und besitzt eine Akkreditierung für das Einweiserportal, stimmen Sie hiermit der Weitergabe Ihrer persönlichen Daten an den einweisenden Arzt zu“. Bei der Vorstellung des Projekts machten wir deutlich, dass dies nicht ausreicht. Zum einen bedarf es einer vorherigen Aufklärung der Patientinnen und Patienten – möglicherweise schon durch den einweisenden Arzt vor dem Krankenhausaufenthalt. Die Aufklärung muss über das Verfahren informieren, u. a. den betroffenen Datenumfang

umschreiben, die Zugriffsdauer festlegen und auf Freiwilligkeit, Wahl- und Widerrufsrechte hinweisen. Die LBK Hamburg GmbH sagte entsprechende Unterlagen zu.

Zum anderen darf im Behandlungsvertrag die Einwilligung in die gewollte Behandlung nicht untrennbar mit der Einwilligung in die – möglicherweise nicht gewollte – Nutzung des Einweiserportals verbunden werden. Der Patient, die Patientin muss vielmehr das Recht erhalten, den Zugriff auf die Krankenhausdaten durch den einweisenden Arzt auszuschließen. Es muss ihm bzw. ihr überlassen bleiben, die Ärzte zu bestimmen, die während und nach dem Krankenhausaufenthalt auf die Patientendaten elektronisch zugreifen können. Dabei wird in der Regel weniger der einweisende Arzt als vielmehr der nachbehandelnde Arzt – der Haus- oder ein Facharzt – in Betracht kommen. Das Hamburgische Krankenhausgesetz lässt selbst eine konventionelle Übermittlung von einzelnen Patientendaten aus dem Krankenhaus „zur Durchführung einer Mit-, Weiter- oder Nachbehandlung" nur zu, „wenn der Patient nach Hinweis auf die beabsichtigte Übermittlung nicht etwas anderes bestimmt" (§ 11). Um so mehr erfordert die Ermächtigung zu einem automatisierten, nicht nur einmaligen und nicht auf ein einzelnes Dokument beschränkten Abruf eine ausdrückliche, gut informierte, schriftliche Einwilligung des betroffenen Patienten. Zu prüfen ist in diesem Rahmen auch, wie weit das Recht des Patienten gehen kann oder soll, den Umfang und die Art der zugriffsfähigen Daten – bis hin zur Selektion einzelner Befunde aus dem Gesamtzusammenhang – selbst zu bestimmen.

Einen anderen Weg geht das UKE: Hier wird mit dem Projekt „EPNET" sowohl ein Portal für Patienten als auch ein Portal für Partner (niedergelassene Ärzte) eingerichtet. Zunächst definiert das Krankenhaus allgemein die Bereiche / Dokumente der elektronischen Patientenakte, die Zugriffen von außen überhaupt geöffnet werden sollen („regelbasierte Voreinstellung"). Hat ein Patient, eine Patientin Interesse daran, über das „Patientenportal" auf die eigenen Behandlungsdaten elektronisch zuzugreifen, schließt das UKE mit ihm / ihr auf der Grundlage ausführlicher Allgemeiner Geschäftsbedingungen einen entsprechenden Nutzungsvertrag. Für Minderjährige gibt es eigene Regelungen. Entwürfe der Geschäftsbedingungen und Verträge liegen uns vor. Neben der Vertragskopie werden dem Patienten ein Infoblatt und eine Nutzungsbeschreibung ausgehändigt.

Für den elektronischen Zugriff erhält der Patient, die Patientin ein Stück Hardware (einen „USB-eToken"), der vorab mit einem Zertifikat „betankt" wurde, und ein Initialpasswort. Zur Freischaltung durch das UKE sind die Vorlage des Personalausweises und der handschriftliche Vermerk der Personalausweisnummer im Vertrag vorgesehen. Nach unserem Hinweis auf das Verbot, Personalausweisnummern für Datenabrufe zu nutzen, verzichtet das UKE auf die Speicherung der Nummer.

Über das Patientenportal kann der Patient auch Dritten (Ärzten, Angehörigen) Zugriff auf die eigenen Krankenhausdaten gewähren. Dies erfolgt – ähnlich dem PIN / TAN-Verfahren beim homebanking – über „Einmal-Logins & Passwörter (ELP)“, die das System auf Initiative des Patienten herstellt, ausdruckt und vom Patienten Dritten überlassen werden.

Das „Partnerportal“ dient dagegen einer regelmäßigen Kommunikation zwischen UKE und externen Ärzten. Mit der Akkreditierung wird der Arzt zunächst gesondert auf Schweigepflicht, Datensicherheitsanforderungen und die Zweckbindung der abgerufenen Daten hingewiesen. Er erhält ein Initialpasswort mit einem Login-Namen und eine spezielle Version eines UKE-Web-Clients, der Client- und Server-Zertifikate zur Authentifizierung und Anmeldung nutzt. Auch die Vergabe eines eToken soll möglich sein.

Ist der Arzt akkreditiert, wird der Patient bei seiner Krankenhausaufnahme über die Möglichkeiten von EPNET aufgeklärt und um seine schriftliche Einwilligung in den Datenzugriff durch den einweisenden Arzt gebeten. Diese Unterlagen liegen zur Zeit noch nicht vor. Der Patient soll den Zugriff des Arztes entweder auf alle voreingestellten Daten eröffnen oder auf den abschließenden Arztbrief beschränken können. Die Möglichkeit einer Einzeldaten-Auswahl erhält der Patient nicht. Bei neuen Informationen zu seinen Patienten wird der externe Arzt-Partner vom Krankenhaus durch eine E-Mail informiert. Diese enthält keinen Patientennamen, sondern nur eine Internetadresse, über die er – mit einer verschlüsselten Verbindung, unter Prüfung des Zertifikats und nach Angabe des Passworts – in die freigegebenen Datenbereiche seiner Patienten gelangt. Der Arzt kann die Daten in seine eigene Praxis-Software übernehmen. Widerruft der Patient die Einwilligung in die Zugriffsberechtigung des Arztes, muss er sich hinsichtlich der bereits übernommenen Daten direkt mit dem Arzt auseinander setzen.

Insgesamt verwenden LBK Hamburg GmbH und UKE – zu Recht – erhebliche Mühen auf die technische Konfiguration einer sicheren und praktikablen elektronischen Zugriffsmöglichkeit. Nach unserer Beratung wurde aber auch die Frage intensiver behandelt, wie der Patient, die Patientin in die Lage versetzt wird, selbst zu bestimmen, welcher Arzt welche Daten zu welchem Zweck und zu welcher Zeit (wie lange) aus dem Krankenhaus abrufen und in die eigene Patientenverwaltung integrieren kann. Ob das Mitspracherecht des Patienten auch die „regelbasierte Voreinstellung“ umfassen sollte, ist noch zu prüfen. Für die zukünftige Einführung der elektronischen Gesundheitskarte sieht das Sozialgesetzbuch V differenzierte Einwilligungs-Bestimmungen vor. Das „Einweiser-“ oder „Partner-Portal“ darf diese gesetzlichen Vorgaben ebenso wenig unterlaufen wie die im Hamburger Krankenhausgesetz und in den Datenschutzgesetzen normierten Patientenrechte auf Bestimmung von Datenempfängern und auf Auskunft zu allen zur Person gespeicherten Daten. Gegebenenfalls sind letztere außerhalb der EDV-Portale zu realisieren.

13.4 Patientenrechte auf Auskunft und Akteneinsicht

Neben dem vertrags- und berufsrechtlich begründeten Patientenrecht auf Akteneinsicht sind vor allem gesetzliche Spezialregelungen zu beachten, die das Patientenrecht oft eindeutiger regeln.

Immer wieder bitten uns Patientinnen und Patienten, sie bei der Durchsetzung ihres Rechts auf Einsicht in Behandlungs- und Untersuchungsunterlagen zu unterstützen. Generell haben Patientinnen und Patienten aus dem Behandlungsvertrag und aufgrund der berufsethischen Pflichten des Arztes grundsätzlich einen Anspruch auf Einsicht in die eigenen Behandlungsunterlagen. Vor allem bei psychiatrischen Behandlungen wird dies jedoch regelmäßig eingeschränkt auf objektive, physische Befunde. Subjektive Bewertungen brauche der Arzt ebenso wenig zu offenbaren wie Tatbestände, deren Kenntnis eine wesentliche Verschlechterung des Gesundheitszustandes des Patienten befürchten lassen („therapeutisches Privileg"). Diese von der Rechtsprechung im Rahmen des Arztrechts geformte Auffassung ist Jahrzehnte alt und berücksichtigt nur unvollkommen das informationelle Selbstbestimmungsrecht der Patienten in seinem heutigen Verständnis. So ist die Trennung von objektiven und subjektiven Befunden gerade im psychiatrischen Bereich äußerst schwierig: Wie ist zum Beispiel eine dokumentierte Verdachtsdiagnose zu bewerten? Aber auch bei Gutachten und Arztbriefen, die an Dritte versandt wurden, oder nach Arztwechsel und Beendigung einer Therapie sind die genannten Einschränkungen des Einsichtsrechts kaum begründbar. In der Praxis führen Nachfragen und Erläuterungen unsererseits gegenüber zunächst zurückhaltenden Ärztinnen und Ärzten in den meisten Fällen zu der vom Patienten gewünschten Einsichtnahme.

In einigen Bereichen ist für die beschriebene einengende Ableitung des Einsichtsrechts aus Vertrag oder Berufspflicht kein Raum: Wo spezialgesetzliche Normen das Auskunfts- und Einsichtsrecht ausdrücklich regeln, ist der Rückgriff auf das allgemeine Arztrecht – einschließlich der genannten Einschränkungen – ausgeschlossen.

In einem uns vorgestellten Fall musste sich ein Berufspilot einer Begutachtung seiner Zuverlässigkeit und Tauglichkeit durch einen flugmedizinischen Sachverständigen unterziehen. Die Einsichtnahme in das – auch psychologische – Gutachten wurde ihm zunächst verweigert. Dabei sieht § 24 c der Luftverkehrszulassungsordnung für derartige Fälle ausdrücklich vor: „Unbeschadet datenschutzrechtlicher Auskunftsrechte erhält der Betroffene auf Verlangen eine Abschrift des Gutachtens". Diese klare Regelung konnte erst nach längerer Prüfung durch die Sachverständigen-Einrichtung durchgesetzt werden.

Aber auch für die vielfach strittigen Einsichtnahmen in Behandlungsunterlagen psychiatrischer Krankenhausabteilungen gibt es in Hamburg eine Spezialnorm: § 32 des Gesetzes über Hilfen und Schutzmaßnahmen bei psychi-

schen Krankheiten (HmbPsychKG) normiert ein generelles Auskunfts- und Einsichtsrecht. Einschränkend wird lediglich festgestellt: „Der psychisch kranken Person können Auskunft und Einsicht versagt werden, wenn eine Verständigung mit ihr wegen ihres Gesundheitszustands nicht möglich ist." Das oben genannte „therapeutische Privileg" wird hier ebenso wenig anerkannt wie im Hamburger Krankenhausgesetz (HmbKHG). Es hat nur insofern einen Niederschlag gefunden, als das Krankenhaus „die Auskunft durch einen Arzt vermitteln lassen (soll), wenn zu befürchten ist, dass die direkte Auskunft erhebliche Nachteile für den Gesundheitszustand des Patienten hätte. Entsprechendes gilt für die Einsicht in die Aufzeichnungen." (§ 13 HmbKHG). Es geht also nur um das Wie, nicht um das Ob der Auskunft und Einsicht. Nur im Hamburgischen Krebsregistergesetz wird ausnahmsweise festgelegt, dass die Auskunft über die im Register gespeicherten Daten „nur einem vom Betroffenen zu benennenden Arzt erteilt" wird. Allerdings schränkt dies das oben genannte eigene Recht der betroffenen Person auf Einsicht der Unterlagen beim behandelnden Arzt oder im Krankenhaus nicht ein.

Schließlich gibt es neben den medizinrechtlichen und spezialgesetzlichen Auskunfts- und Einsichtsregelungen auch noch das datenschutzrechtliche Auskunftsrecht. Gegenüber staatlichen Einrichtungen in Hamburg ist es in § 18 HmbDSG, gegenüber niedergelassenen Ärzten ist es in § 34 BDSG geregelt. Es bezieht sich auf alle zu einer Person gespeicherten Daten einschließlich des Zwecks der Speicherung, der Herkunft der Daten und regelmäßiger Übermittlungsempfänger. Es geht damit im Umfang über die reinen Behandlungsdaten hinaus, setzt aber im nicht öffentlichen Bereich voraus, dass die ärztlichen Dokumentationen in Dateien und nicht in einzelnen Akten geführt werden.

Insgesamt bemühen wir uns, den Ärztinnen und Ärzten deutlich zu machen, dass die Wahrnehmung der Patientenrechte auf Auskunft und Einsicht in die Krankenakte nicht als Vertrauensbruch empfunden, sondern zum Anlass für ein Gespräch genutzt werden sollte. In Zeiten scheinbar grenzenloser Information durch Internet und Selbsthilfegruppen müssen sich Ärztinnen, Ärzte und Krankenhäuser auch auf Patientinnen und Patienten einstellen, die eine vollständige Information über alle über sie gesammelten Daten einfordern.

14. Forschung

14.1 Prüfung des Forschungslabors der UKE-Klinik für Allgemeinchirurgie

Gravierende Mängel bei der Patienteneinwilligung sowie bei der Organisation der elektronischen Tumorbank wurden nach unserer Datenschutzprüfung gründlich und zügig behoben.

Im Mai 2005 prüften wir die Proben- und Datenbank und die Organisation des Forschungslabors der Klinik für Allgemein-, Viszeral- und Thoraxchirurgie im Universitätsklinikum Hamburg-Eppendorf (UKE). Patientinnen und Patienten, die in dieser Klinik operiert werden, erhalten zuvor eine Einwilligungserklärung mit Erläuterung zur Unterschrift vorgelegt, mit der sie um Blut- und / oder Gewebeproben für Forschungszwecke gebeten werden. Diese Erklärungen entsprachen in keiner Weise den datenschutzrechtlichen Anforderungen: Sie unterschieden nicht zwischen der Einwilligung in den körperlichen Eingriff zur Probenentnahme und der Einwilligung in die Probennutzung und Datenverarbeitung. Den Formblättern war nicht klar zu entnehmen, ob mit Tumorgewebe geforscht werden soll, das zu Behandlungszwecken entfernt wurde („Behandlungsproben"), oder mit Proben, die zusätzlich nur für Forschungszwecke entnommen wurden („Forschungsproben"). Die Erklärungen differenzierten auch nicht zwischen aktuellen konkreten und befristeten Forschungsprojekten einerseits und der Sammlung von Proben in einer Biobank für noch unbestimmte zukünftige Forschung andererseits. Schließlich war die Einwilligung in die Forschung untrennbar verbunden mit der Einwilligung in die Meldung zum Krebsregister.

Alle diese Defizite der Aufklärung und Einwilligung wurden inzwischen behoben. Die betriebliche Datenschutzbeauftragte des UKE entwickelte zusammen mit der Klinik und uns ein Set von drei Informations- und Einwilligungsmustern, von denen dem Patienten je nach konkreter Situation und Forschungsplanung jeweils nur eine Fassung zur Unterschrift ausgehändigt wird. Die Einwilligungen in die zusätzliche Probenentnahme für ein konkret zu umschreibendes Forschungsprojekt bzw. für die allgemeine Biobank werden ausdrücklich verbunden mit einer gesonderten Einwilligung in die Nutzung von Behandlungsproben(resten). Ist eine zusätzliche Probenentnahme für Forschungszwecke nicht vorgesehen, wird der Patient um die Einwilligung in die Aufnahme der Behandlungsproben(reste) in die Biobank gebeten. Die Einwilligung in die Meldung zum Krebsregister ist an dieser Stelle entfallen.

Während die einzelnen Proben nur mit Labornummern gekennzeichnet sind und sicher aufbewahrt werden, verstießen Datenverwaltung und elektronische Tumordatenbank ebenfalls – zum Teil in grober Weise – gegen Datenschutzanforderungen: Im Labor wurden verschiedene Ordner, Kladden und Dokumente verwahrt, die nicht nur die Labornummern der Proben und klinischen Daten enthielten, sondern auch die dazu gehörenden Patientennamen im Klartext. Dasselbe galt für die elektronische Tumorbank. Sie wurde zwar auf einem stand-alone-PC geführt. Dieser stand jedoch – ohne Passwortschutz – jeder Mitarbeiterin, jedem Mitarbeiter des Labors, insbesondere den verschiedenen Doktoranden, in vollem Umfang zur Verfügung. Jede / r hatte nicht nur Zugriff auf die – mit den Patientennamen verbundenen – Proben- und klinischen Daten der Tumorbank, sondern auch auf Auswertungen und Projektdarstellungen der Kolleginnen und Kollegen. Darüber hinaus waren auf dem ungeschütz-

ten Rechner neben der Tumorbank verschiedene personenbezogene Dokumente mehrerer Doktoranden und des Chefarztes gespeichert. Besonders kritisch war eine Sammlung von patientenbezogenen Arztbriefen mit höchst sensiblen Daten seit 1996. Auch auf sie konnte jeder Doktorand zugreifen.

Auf eine formelle Beanstandung haben wir nur deshalb verzichtet, weil die erkannten Mängel umgehend beseitigt wurden. Inzwischen werden Patientennamen ausschließlich im Behandlungsbereich der Klinik verarbeitet. In das Forschungslabor gelangen nur noch pseudonymisierte Daten – sowohl in Papierform als auch elektronisch. Soweit Forscher mit einzelnen Patienten Kontakt aufnehmen oder verschiedene Datenquellen demselben Patienten zuordnen müssen und dafür die Identität eines Patienten benötigen, erfolgt die Entschlüsselung durch eine Studienfachkraft (study-nurse), die in einem eigenen Arbeitsraum im Klinikbereich eine Schlüsselliste (Namen / Labornummer) verwaltet. Der PC, auf dem nur noch die – pseudonymisierte – Tumorbank geführt wird, ist nun passwortgeschützt. Jeder Nutzer kann über eine eigene Kennung nur auf den eigenen Datenbestand und die eigene Auswertung zugreifen.

Bisher gibt es keine einheitliche UKE-weite Regelung für die Proben- und Datenverwaltung in den Behandlungs- und Forschungsabteilungen der Kliniken. In früheren Prüfungen haben wir vielmehr erfahren, dass dafür sehr unterschiedliche Strukturen und Verfahren angewandt werden. Aus unserer Sicht würde eine übergreifende Regelung in Form einer verbindlichen Verfahrensanweisung des UKE-Vorstands nicht nur den Datenschutz der Patientinnen und Patienten deutlich verbessern, sondern könnte zugleich als Qualitätsmerkmal im internationalen Forschungswettbewerb genutzt werden. Wir werden weiter auf eine solche generelle Regelung hinwirken.

14.2 Beratung von Forschungsprojekten – Übersicht

Durch die Beratung von mehreren Forschungsvorhaben konnten wir den Datenschutz für die betroffenen Probanden verbessern.

Anders als die Ethik-Kommission der Ärztekammer ist der Hamburgische Datenschutzbeauftragte vor Durchführung eines Forschungsprojekts „am Menschen“ nicht regelhaft zu beteiligen. Werden für das Forschungsprojekt allerdings personenbezogene Daten aus dem Krebsregister benötigt, hat die Behörde für Wissenschaft und Gesundheit vor ihrer Entscheidung den Hamburgischen Datenschutzbeauftragten „anzuhören“. Auf diese Weise erhalten wir regelmäßig Kenntnis von den entsprechenden Studienkonzepten und nutzen dies für datenschutzrechtliche Stellungnahmen. Wollen öffentliche Stellen – außer Krankenhäusern – (z. B. Gesundheitsämter) personenbezogene Daten für ein bestimmtes Forschungsvorhaben an Dritte übermitteln, so ist diese Entscheidung ebenfalls dem Hamburgischen Datenschutzbeauftragten mitzuteilen, § 27 Abs. 2 HmbDSG. Im Übrigen befassen wir uns mit einzelnen

Forschungsprojekten, wenn die Wissenschaftler uns um eine Beratung bitten – manchmal aufgrund einer entsprechenden Auflage der Ethik-Kommission. Bei überregionalen Studien, die Daten in verschiedenen Bundesländern erheben wollen, werden wir entweder vorab von der koordinierenden Zentralstelle – z. B. dem Robert-Koch-Institut (RKI) in Berlin – oder von den Daten liefernden Hamburger Stellen – z. B. einem bezirklichen Gesundheitsamt – um eine Stellungnahme gebeten. Hier bedarf es auch einer Abstimmung mit den Datenschutzkollegen in den anderen Bundesländern.

Im Berichtszeitraum hatten wir uns mit folgenden überregionalen Forschungsvorhaben zu befassen:

- Kompetenznetz Herzinsuffizienz
- RKI-Studie „Todesfälle bei Kindern im 2.-24. Lebensmonat
- Internationale Studie über das Krebsrisiko bei Asphaltarbeitern.

Aus dem UKE, anderen Universitäts-Fachbereichen, der Hochschule für angewandte Wissenschaften und einzelnen Behörden wurden folgende Forschungsprojekte an uns herangetragen:

- Mobilitätsrestriktionen in Alten- und Pflegeheimen
- Früherkennung von Erkrankungen der Brust
- Ernährung bei Kleinkindern unter 3 Jahren
- Krankheitskonzepte von Patienten mit Hypertonie
- Lassen sich Phänomene der Nicht-zur-Kenntnisnahme evidenzbasierter Verbraucherinformationen mit der Theorie der kognitiven Dissonanz erklären?
- Optimierung von Arbeitsprozessen mit der Pimex-Methode
- Biomonitoring aromatischer Amine im Urin bei Nichtrauchern und Rauchern
- Suizidalität im Psychiatrischen Notdienst und in der Einweisungspraxis der Sozialpsychiatrischen Dienste
- Beratung von Migrantinnen und Migranten in Institutionen der Altenhilfe
- Fentanyl-Studie (Prüfung der Konzentration eines opiathaltigen Schmerzmittels in Haar und Blut von Verstorbenen)
- Stillförderung durch Stressprävention bei werdenden Eltern.
- Evaluierung der Neustrukturierung der Notfallversorgung von Patientinnen und Patienten mit akutem Herzinfarkt in Hamburg
- Wirksamkeit der stationären medizinischen Rehabilitation bei Patienten mit chronischen Rückenschmerzen
- Schwangerschaftsabbrüche bei minderjährigen Frauen

- Evaluationsstudie: Entstigmatisierung von Demenzerkrankungen in der hausärztlichen Praxis
- Quartiersdiagnose Lenzsiedlung anhand der Daten der schulärztlichen Eingangsuntersuchung
- Ambulante neurologische Rehabilitation und Nachsorge bei schädel-hirntraumatisierten Kindern und Jugendlichen
- Fallstudien: Kriterien sozialer Ungleichheit und deren Auswirkung auf den Zugang zum Gesundheitswesen
- Register älterer Tumorpatienten.

Bei der Beratung ging es in erster Linie um die Sicherstellung einer anonymen oder pseudonymen Datenverarbeitung und um die Formulierung von Aufklärungs- und Einwilligungstexten. In allen Fällen konnten datenschutzrechtliche Verbesserungen erreicht werden, ohne dass das Forschungsvorhaben beeinträchtigt wurde.

14.3 Zusammenarbeit mit der Ethik-Kommission der Ärztekammer

Um Doppelarbeit und inhaltliche Differenzen zu vermeiden, klärten wir mit der Ethik-Kommission den jeweiligen Aufgabenzuschnitt und die datenschutzrechtlichen Mustertexte für Forschungsprojekte.

Bei der Beratung und Prüfung medizinischer Forschungsprojekte hielten uns einzelne betroffene Wissenschaftler entgegen, dass sie sich an die datenschutzrechtlichen Aufklärungs- und Einwilligungs-Mustertexte der Ethik-Kommission gehalten hätten bzw. die Ethik-Kommission das Projekt bereits genehmigt habe. Wir suchten daraufhin den Kontakt zur Ethik-Kommission, um Verfahrensfragen abzustimmen und Differenzen zu klären.

In einem Gespräch mit dem Vorsitzenden, der Geschäftsführerin und weiteren Mitgliedern der Ehtik-Kommission steckten wir die jeweiligen Aufgabenkreise und ihre Überschneidungsbereiche ab:

Die Ethik-Kommission geht davon aus, dass ihr alle medizinischen Forschungsprojekte „am Menschen“ – einschließlich retrospektiver Aktenauswertungen und der Einrichtung von Probenbanken für zukünftige Forschungsprojekte – vorzulegen sind. Die Kommission vertritt dazu die Auffassung, sie habe zu allen ethischen und rechtlichen Gesichtspunkten (einschließlich des Datenschutzes) Stellung zu nehmen. Fragen der technischen Datensicherheit sollten die Forscherinnen und Forscher dagegen nur mit dem Datenschutzbeauftragten klären. Wir verwiesen demgegenüber auf die gesetzliche Pflicht öffentlicher Stellen (z. B. des UKE), Entscheidungen über personenbezogene Datenübermittlungen zu Forschungszwecken dem Hamburgischen Datenschutzbeauftragten mitzuteilen (§ 27 Abs. 2 HmbDSG). Auch bei der personenbezogenen Datenübermittlung aus dem Krebsregister zu Forschungszwecke

sind wir zu beteiligen (§ 9 Abs. 2 HmbKrebsregisterG). Dabei obliegt uns nicht nur eine Beratungsaufgabe, sondern auch ein Prüfungs- und Kontrollrecht, das nicht von einem Antrag der Forscherinnen und Forscher abhängt.

Angesichts dieser Rechtslage verständigten wir uns darauf, dass die Ethik-Kommission ihre im Internet bereitgestellten Muster-Texte zum Datenschutz unter Berücksichtigung unserer Empfehlungen modifiziert. Hierbei geht es um Präzisierungen hinsichtlich einzelner Rechtsvorschriften, um Fragen der „Pseudonymisierung“ und „Anonymisierung“ sowie um die Reichweite des grundsätzlichen Einwilligungserfordernisses bei medizinischen Forschungen.

Die Forschungsklauseln des Hamburgischen Krankenhausgesetzes und des Hamburgischen Datenschutzgesetzes ermöglichen – bei Vorliegen bestimmter Voraussetzungen – die Zulassung wissenschaftlicher Studien ohne eine Einwilligung der Betroffenen. Die hier meist notwendige Abwägung zwischen dem Forschungsinteresse und dem Individualinteresse der Probanden nutzt die Ethik-Kommission nach eigenen Angaben zur prinzipiellen Forderung nach einer individuellen Einwilligung, wo immer es möglich ist. Nicht zu entscheiden hatten wir die Frage, inwieweit die Ethik-Kommission dadurch gegenüber Forschern ausdrückliche gesetzliche Ermächtigungen einschränken könne.

Ein weiterer Gesprächsgegenstand war die Einrichtung von Biobanken, also die Sammlung von Proben und Daten für noch unbestimmte zukünftige Forschungen. Hier ging es um die fehlende konkrete Zweckbestimmung, um die notwendige Unbestimmtheit der einzuholenden Einwilligung sowie um die zukünftig immer leichter werdende Re-Identifizierung von Probanden über den Abgleich genetischer Analyseergebnisse. Müssen deswegen Ethik-Kommission und Datenschutzbeauftragter jede einzelne Weitergabe von (Teil-)Proben und Daten aus der Biobank an externe Forscher erneut prüfen? Die Ethik-Kommission teilte unsere Auffassung, dass dies nicht notwendig ist. Die vorangehende Prüfung der Biobank selbst, ihrer Organisation, Datenerhebung und Speicherung sowie die notwendige Pseudonymität bzw. Anonymität der Proben und Daten lassen eine Weitergabe ohne erneute Prüfung vertretbar erscheinen – jedenfalls zurzeit noch. Dies auch vor dem Hintergrund, dass das Forschungsvorhaben des externen Dritten seinerseits der zuständigen Ethik-Kommission und ggf. auch dem Datenschutzbeauftragten zur Begutachtung vorzulegen ist.

Mit der Ethik-Kommission wurde vereinbart, dass die Forscherinnen und Forscher im Übrigen möglichst frühzeitig auf die Aufgaben und Leistungen der jeweils anderen Institution hingewiesen werden.

14.4 Einwilligung in Forschungsvorhaben

Veränderungen in der Forschungslandschaft wirken sich auf die bisher bewährten Anforderungen des Datenschutzes zum Schutz der Probanden-Selbstbestimmung aus.

Unsere Beratung von Forscherinnen und Forschern bezieht sich zumeist auf medizinische Forschung im UKE. Dafür gilt die Forschungsklausel des § 12 des Hamburgischen Krankenhausgesetzes (HmbKHG): Behandelnde Ärzte dürfen ohne Einwilligung des Patienten mit deren Daten forschen. Forschen andere Personen (z. B. Doktoranden) in demselben Krankenhaus, in dem der Patient behandelt wird bzw. wurde, ist dies ebenfalls ohne dessen Einwilligung zulässig, wenn „schutzwürdige Interessen der Betroffenen nicht gefährdet werden". Selbst eine Übermittlung von personenbezogenen Patientendaten an forschende Dritte ist ohne Einwilligung zulässig, wenn „das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Interessen der Betroffenen erheblich überwiegt" und nicht anders realisiert werden kann. Dieselbe Abwägungsklausel verwendet § 27 HmbDSG für alle anderen Forschungsprojekte, für die keine spezialgesetzlichen Regelungen greifen.

In der Praxis werden diese weiten, eine Abwägung erfordernden Möglichkeiten einer Forschung ohne Einwilligung nur selten genutzt. Die Leitung des UKE geht – auch aus Image- und Wettbewerbsgründen – prinzipiell davon aus, dass Forschung ausschließlich auf einer Einwilligung der Patienten beruhen sollte. Auch die Ethik-Kommission der Hamburger Ärztekammer ist der Auffassung, dass für die gesetzlichen Ermächtigungen zur Forschung ohne Einwilligung eigentlich kein Raum ist. Schließlich hat auch die Dienststelle des Hamburgischen Datenschutzbeauftragten bisher sehr konsequent gefordert, dass die Probanden umfassend aufgeklärt werden und im Einzelnen – zumeist schriftlich – zustimmen müssen, wenn mit ihren Proben und Daten geforscht werden soll.

Inzwischen müssen wir in der Forschungslandschaft einige Veränderungen feststellen, die Anlass geben, über den bisherigen Konsens für eine absolute Priorität der Einwilligung neu nachzudenken:

- Alle Forschungsklauseln und auch die herkömmlichen Forschungseinwilligungen beziehen sich auf konkrete zeitlich befristete Forschungsvorhaben, die klar umschrieben werden können. Die Entwicklung zur Sammlung von Proben und Daten in Biobanken für noch unbestimmte zukünftige Forschungszwecke wird davon nicht erfasst. Die von den Probanden hierfür erbetene Einwilligung bleibt notwendig sehr vage, die betroffene Person kann nicht wirklich abschätzen, auf was genau sie sich mit ihrer Einwilligung einlässt. Die üblichen datenschutzrechtlichen Anforderungen an eine Einwilligung, wie sie etwa in § 5 HmbDSG oder in § 7 Abs. 2 HmbKHG festgelegt werden, können nicht erfüllt werden.
- Forschung ist zunehmend vernetzt. Datenerhebungen und Datenverarbeitungen werden auf mehrere Bundesländer oder sogar international verteilt (sog. Multi-Center-Studien), nicht selten mit verschiedenen Koordinationsstellen für Teilfunktionen des Projekts. Beispiele sind etwa die verschiedenen über die ganze Bundesrepublik verteilten „Kompetenznetze" in der

medizinischen Forschung. Nicht zuletzt die datenschutzrechtlichen Forderungen haben dabei zu sehr komplexen Kommunikationsbeziehungen mit mehrfachen Pseudonymisierungen, getrennten Datenbanken und aufwändigen Re-Identifizierungsverfahren geführt. Selbst Fachleute sind kaum in der Lage, alle Aspekte der Datensicherung und des Datenschutzes in diesen Netzen zu übersehen. Wie sollen diese für die Einwilligungsentscheidung durchaus wichtigen Strukturen den Patientinnen und Patienten in der geforderten „umfassenden Aufklärung" vermittelt werden?

- Medizinische Forschung ist zunehmend genetische Forschung. Gerade die Datenschutzbeauftragten – und wir in Hamburg haben hier eine gewisse Vorreiterrolle gespielt – haben die besondere Qualität und das Gefährdungspotenzial der Verarbeitung genetischer Daten für die informationelle Selbstbestimmung seit langem erkannt und betont. Gefordert wurden deshalb gesetzlich festgelegte sehr detaillierte Kataloge für die Gegenstände der Aufklärung und Einwilligung. Inzwischen ist nicht mehr so eindeutig, was eigentlich „genetische Forschung" ist. So zählt der Arbeitsentwurf eines Gendiagnostikgesetzes auch Untersuchungen des „Phänotyps" (der äußerlich wahrnehmbaren Merkmale wie z. B. Rot-Grün-Blindheit) zu den „genetische Untersuchungen", wenn sie Rückschlüsse auf die Erbsubstanz zulassen. Im Klinikalltag sind heute zudem molekulare und Genprodukt-Untersuchungen zur Ermittlung oder Bestätigung einer Krankheits-Diagnose Routine. Ist es im Interesse der Patienten, wenn auch hier die stark erhöhten Anforderungen an Aufklärung und Einwilligung durchgesetzt werden?
- Anlässlich eines uns vorgelegten Forschungsprojekts aus dem Bildungsbereich sei schließlich noch auf einen anderen Aspekt hingewiesen: Zumindest in Großstädten wie Hamburg gehören Ausländerinnen und Ausländer mit schwachen Deutschkenntnissen und einem eigenen kulturellen Hintergrund zum repräsentativen Bevölkerungsdurchschnitt. Eine Umsetzung der bewährten Datenschutzanforderungen an Aufklärung und Einwilligung im Forschungsbereich ist ihnen gegenüber praktisch nicht möglich. Von einer freiwilligen informierten Einwilligung kann in der Regel nur dann ausgegangen werden, wenn die Kommunikation in der Muttersprache erfolgt – bei Projekten mit Probanden aus verschiedenen Nationen ist dies kaum zu gewährleisten.

Die vorstehenden Überlegungen sind als Problemanzeige zu verstehen, die die Erfahrung aus unserer Beratungs- und Prüfungstätigkeit widerspiegelt. Eine Alternative kann darin bestehen, die gesetzlichen Forschungsermächtigungen wieder in den Blick zu nehmen und zu nutzen. Im Vordergrund der Betrachtung sollte das Prinzip der weitgehenden Trennung von Behandlungs- und Forschungsbereichen in Universitätskliniken, die Forderung nach einer in aller Regel anonymen oder sicher pseudonymen Forschung und das Gebot, geeignete Informationen für die Probanden zumindest anzubieten, stehen. Die Datenschutzbeauftragten müssen vermeiden, das Grundrecht auf informatio-

nelle Selbstbestimmung in einer Weise durchzusetzen, die an der realen Entwicklung und an den tatsächlichen Bedürfnissen der Grundrechtsträger weitgehend vorbei geht. Es kann nicht unser Ziel sein, Patienten und Probanden durch (zu) ausführliche Aufklärungs- und Einwilligungstexte zu verunsichern und vor einer Teilnahme an wissenschaftlicher Forschung abzuschrecken.

Wir haben deswegen ein Grundsatzpapier „Datenschutzrechtliche Einwilligungen in medizinische Forschung – Selbstbestimmung oder Überforderung des Patienten?“ dem Bund-Länder-Arbeitskreis Wissenschaft der Datenschutzbeauftragten zur Erörterung übermittelt. Darin schlagen wir vor, – jenseits der geltenden gesetzlichen Ermächtigung zur Patientendatenverarbeitung für Forschungszwecke – die komplizierten Informations- und Einwilligungserklärungen durch Regelwerke der Wissenschaft zu ersetzen, die der Gesetzgeber für verbindlich erklärt. Dann kann der Patient auf eine datenschutzgerechte Durchführung der medizinischen Forschung vertrauen und sich auf eine eher allgemeine Einwilligung in die Nutzung seiner Proben und Daten zu Forschungszwecken beschränken.

15. Medien / Telekommunikation

15.1 Gebühreneinzugszentrale GEZ

Die Datenschutzbeauftragten legen Änderungsvorschläge vor zu den neu eingeführten Regelungen der Gebührenbefreiung und der Ermächtigung der GEZ, sich am Adresshandel zu beteiligen.

Der 8. Rundfunkänderungsstaatsvertrag, der 2005 von den Länderparlamenten angenommen wurde, enthält unter anderem folgende Modifikationen des Rundfunkgebührenstaatsvertrages:

- Die Befreiung von Rundfunkgebühren wegen Bedürftigkeit ist nicht mehr bei den einzelnen Sozialdienststellen zu beantragen, sondern direkt bei der Gebühreneinzugszentrale der Rundfunkanstalten (GEZ). Dazu ist der GEZ – im Original oder in beglaubigter Kopie – der vollständige Leistungsbescheid für Arbeitslosengeld II, Sozialhilfe oder ähnliches vorzulegen. Mit diesen Bescheiden erhält die GEZ viele sensible Daten über sozial schwache Rundfunkteilnehmer, die über die erforderliche Information der Bedürftigkeit weit hinausgehen. Die GEZ speichert diese Daten vollständig und in digitalisierter Form bei den Teilnehmerkonten. Sie erhält damit einen Sozialdatenbestand über alle sozial schwachen Rundfunkteilnehmer der Bundesrepublik.
- Es wurde ausdrücklich geregelt, dass die GEZ, „zur Feststellung, ob ein Rundfunkteilnehmerverhältnis vorliegt, oder im Rahmen des Einzugs der Rundfunkgebühren entsprechend § 28 Bundesdatenschutzgesetz“ ge-

kaufte Adressbestände mit den eigenen Dateien abgleichen darf. Durch diese Verweisung werden die öffentlich-rechtlichen Rundfunkanstalten und die GEZ als ihre Auftragsdatenverarbeiterin völlig systemwidrig zur Teilnahme am Adresshandel zugelassen, den das BDSG sonst nur privaten, nicht öffentlichen Stellen vorbehält. Dadurch ist es der GEZ möglich, etwa aus der Tatsache des Abonnements einer Programmzeitschrift Anhaltspunkte zu gewinnen, ob eine Person ein Rundfunkgerät nutzt, ohne es angemeldet zu haben. Daneben bleiben die (öffentlich-rechtlichen) Meldedatenübermittlungen an die GEZ ausdrücklich erhalten.

Zur Verbesserung des Datenschutzes sind die Landesdatenschutzbeauftragten überein gekommen, es nicht bei diesen „verunglückten" Regelungen im Rundfunkgebührenstaatsvertrag zu belassen, sondern den Rundfunkreferenten der Länder konkrete Änderungen vorzuschlagen:

Zur Entscheidung über die Gebührenbefreiung sollte die GEZ künftig nicht mehr den vollständigen Bescheid des Sozialleistungsträgers erhalten, sondern nur noch eine offizielle Bestätigung dieser Stellen mit eventuell notwendigen weiteren Angaben wie etwa der Gültigkeitsdauer des Bescheides. Dies ließe sich durch die Umgestaltung der Sozialleistungsbescheide erreichen, die um eine kurz gefasste Bestätigung für die GEZ ergänzt werden müssten. Diese abzustempeln wäre für die Sozialdienststelle nicht aufwändiger als die Beglaubigung einer vollständigen Kopie.

Hinsichtlich der Teilnahme der GEZ am Adresshandel mussten die Datenschutzbeauftragten erkennen, dass die Staats- und Senatskanzleien sowie die Rundfunkanstalten nicht bereit sind, die seit Jahren gepflegte und nun sanktionierte Praxis der GEZ einzuschränken. Statt des Systembruchs – der Vermischung von öffentlich-rechtlicher Trägerschaft mit privat-rechtlichen Befugnissen – schlagen die Datenschutzbeauftragten daher eine eigenständige Vollregelung für Adressdatenabgleiche durch die GEZ im Gebührenstaatsvertrag ohne Verweisung auf das Bundesdatenschutzgesetz vor. In dieser Regelung können dann die Zweckbestimmung präzisiert, die Art und Qualität der Adressdaten näher umschrieben, ihr Umfang begrenzt und Rückmeldungen an die Adresshändler ausgeschlossen werden.

Auch wenn wir diese Vorschläge nicht als datenschutzrechtliches Optimum, sondern eher als kleineres Übel ansehen, haben wir uns zur Verbesserung der gegenwärtigen Rechtssituation an der Formulierung beteiligt. Die Reaktion der Staats- und Senatskanzleien, Rundfunkanstalten sowie Sozialbehörden bleibt anzuwarten.

15.2 Vorratsdatenspeicherung von Telefon- und Internetdaten

In gemeinsamen Entschließungen der Datenschutzbeauftragten teilen wir die Kritik an den EU-Beschlüssen, die Telekommunikationsanbieter zu verpflichten, Telefon- und Internetverbindungsdaten auf Vorrat zu speichern.

Während der Deutsche Bundestag bei der Änderung des Telekommunikationsgesetzes 2004 eine Vorratsspeicherung von Verbindungsdaten für die Sicherheitsbehörden ausdrücklich abgelehnt hatte, setzten sich 2004 der Europäischen Rat (die Innenminister der Mitgliedsländer) und 2005 auch die EU-Kommission und das EU-Parlament für eine solche Verpflichtung der Telekommunikationsanbieter ein:

Der Entwurf für einen Rahmenbeschluss des Rats beschreibt die betroffenen Datenarten, legt eine Speicherfrist von ein bis höchstens 3 Jahren fest und bestimmt als Zweck die „Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus".

Die EU-Kommission legte in ihrem Entwurf einer EU-Richtlinie die betroffenen Verkehrs- und Standortdaten in der Festnetz-, Mobilfunk- und Internet-Kommunikation im Einzelnen fest und sah eine Speicherfrist von 1 Jahr für die Telefon- und 6 Monaten für die Internet-Verbindungsdaten vor. Ziel sei die „Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten wie Terrorismus und organisierter Kriminalität". Ferner regelt der Entwurf eine Entschädigungspflicht zugunsten der Anbieter.

Am 14. Dezember 2005 beschloss das EU-Parlament die Richtlinie in einer abgeänderten Fassung. Danach können die Mitgliedsländer eine Speicherfrist zwischen 6 Monaten und 2 Jahren festlegen. Der Zweck, für den diese Daten von den Sicherheitsbehörden genutzt werden dürfen, wurde erweitert und die Entschädigungspflicht des Staates für die Vorhaltung der technischen Infrastruktur durch die Telekommunikationsanbieter wurde gestrichen.

Die Datenschutzbeauftragten hatten sich in der Vergangenheit mehrfach kritisch mit diesen Bestrebungen auseinander gesetzt. Eine „flächendeckende" Vorratsspeicherung von Daten, die für betriebliche und Abrechnungszwecke nicht mehr erforderlich sind, aber das Kommunikationsverhalten von Millionen völlig unverdächtiger Bürgerinnen und Bürgern festhalten, verstößt gegen den Grundsatz der Verhältnismäßigkeit. Die anlasslose Speicherung in dieser Dimension verletzt das Fernmeldegeheimnis des Art.10 Grundgesetz, der nicht nur die Inhalte von privaten Gesprächen schützt, sondern auch ihre näheren Umstände wie Gesprächspartner, Ort, Zeit, Dauer und Art der Kommunikation. Berührt wird darüber hinaus der in der Europäischen Menschenrechtskonvention garantierte Schutz der Privatsphäre. Wie das Bundesverfassungsgericht in seinem Volkszählungsurteil beschrieb, bedroht eine anlasslose Verhaltensbeobachtung und -registrierung die Entschlussfreiheit des Einzelnen, von seinen Grundrechten auf Meinungsäußerung und auf ungehinderte Unterrichtung aus allgemein zugänglichen Quellen Gebrauch zu machen.

Schon im September 2002 fasste die Datenschutzkonferenz eine Entschließung, um einen Vorstoß des Bundesrats zur Vorratsdatenspeicherung zu ver-

hindern. Im Juni 2004 veröffentlichten die Datenschutzbeauftragten eine Presseerklärung zu ersten Überlegungen des EU-Ministerrats. In der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2005 wurde erneut eine gemeinsame Entschließung gefasst. Die Erklärung unterstreicht noch einmal die verfassungsrechtlichen Bedenken gegen eine anlasslose Vorratsspeicherung von Verbindungsdaten und weist darauf hin, dass Mittel mit geringerer Eingriffstiefe wie das in den USA praktizierte kurzfristige „Einfrieren" der Daten im Falle eines konkreten Anlasses bisher nicht ernsthaft geprüft wurden.

Auch in Hamburg wird eine ganze Reihe von Telekommunikationsanbietern und Internet-Providern von der Umsetzung der genannten EU-Richtlinie betroffen. Wir werden uns dafür einsetzen, dass erforderlichenfalls vom Bundesverfassungsgericht geklärt wird, ob die EU-Richtlinie mit dem im Grundgesetz garantierten Schutz der Grundrechte vereinbar ist.

16. Ausländerwesen

16.1 Stichprobenprüfung bei Zugriffen auf die Ausländerdatei

Die Umsetzung des vereinbarten Stichprobenverfahrens nach § 3 Abs. 3 der Ausländerdatenverarbeitungsverordnung bedarf weiterer Nachbesserungen in der technischen und organisatorischen Ausgestaltung.

Über das Stichprobenverfahren in der Ausländerdatenverarbeitung haben wir schon mehrfach berichtet (vgl. insb.19.TB, 12.2). Zuletzt hatten wir dafür mit der Ausländerbehörde ein wesentlich reduziertes Verfahren vereinbart, das aber zugleich die Nachvollziehbarkeit der Zugriffe im Einzelfall besser gewährleisten sollte. Kern der Vereinbarung war, dass die Sachbearbeiter den Anlass und die durchgeführten Maßnahmen so konkret wie möglich beschreiben und die Vorgesetzten die Kontrollen kurzfristig vornehmen und revisionssicher dokumentieren sollten, auch unter Ergänzung unklarer Angaben.

Wir haben das Verfahren im Herbst 2005 in zwei Abschnitten der Ausländerabteilung sowie in zwei Bezirksämtern (Ausländerabteilung und Rechtsamt) geprüft. Es wurde deutlich, dass die Technikunterstützung noch nicht ausreicht und die fachliche Durchführung der Zugriffskontrollen bisher von sehr unterschiedlicher Qualität war.

Wir streben daher in einem erneuten Vorstoß in Zusammenarbeit mit den anwendenden Behörden an, das Verfahren so zu überarbeiten, dass eindeutige, aussagefähige und nachprüfbare Angaben gemacht und die Kontrollen technisch unterstützt dokumentiert werden.

16.2 Lesender Zugriff der Polizei auf die Ausländerdatei

Im Rahmen polizeilicher Ermittlungsverfahren kann ein lesender Zugriff auf die automatisierte Ausländerdatei nur in einem abgestuften Verfahren erfolgen, das die Schwere der Delikte einerseits und die Sensibilität der Daten andererseits in einem angemessenen Verhältnis berücksichtigt.

Im Frühjahr 2005 haben Polizei und Verfassungsschutz das Anliegen an uns herangetragen, einen lesenden vollinhaltlichen Zugriff auf die gemeinsame Ausländerdatei der zentralen Ausländerabteilung und der bezirklichen Ausländerdienststellen zu erhalten.

Ziel der Polizei ist es, über den – inhaltlich unstreitigen – Bereich des Terrorismus hinaus auch in Haftsachen und zur Bekämpfung der allgemeinen Ausländerkriminalität einen schnelleren, aktuelleren und umfangreicheren Zugriff auf benötigte Informationen zu erhalten, als dies bisher mit der Abfrage im bundesweiten Ausländerzentralregister und mit der Einsichtnahme in die einzelne Ausländerakte möglich ist.

Mit dem Zugriff im automatisierten Abrufverfahren wird eine neue Qualität des polizeilichen Zugriffs auf Ausländerdaten eröffnet. Die Ausländerdatei verfolgt mit der Unterstützung der reinen Ausländerverwaltung einen grundlegend anderen Zweck als die Kriminalitätsverfolgung und beinhaltet viele Angaben, die der Polizei über das bundesweite Ausländerzentralregister gar nicht oder zumindest bewusst nicht im automatisierten Abruf zur Verfügung gestellt werden.

Wir halten daher ein abgestuftes Abrufverfahren für erforderlich, nach dem die Straftat umso schwerwiegender sein muss, je mehr Daten abrufbar sein sollen. Je weniger schwerwiegend der Tatvorwurf, desto zurückhaltender sollte der Zugriff sein. Nach diesem Maßstab halten wir einen weitgehenden Zugriff im Rahmen der Bekämpfung des Terrorismus und der organisierten Kriminalität für vertretbar; zur Bekämpfung der allgemeinen Kriminalität sollte ein begrenzter Zugriff auf die Ausländerdatei ausreichen. Entsprechend der Zweckdurchbrechung sind erhöhte Anforderungen an die Protokollierung und die Prüfung der Zulässigkeit der Abrufe zu stellen. Hier haben wir empfohlen, sich an den schon bestehenden Anforderungen der Meldedatenübermittlungsverordnung zu orientieren.

Für dieses automatisierte Abrufverfahren für die Polizei bedarf es darüber hinaus nach § 11 des Hamburgischen Datenschutzgesetzes einer Rechtsverordnung des Senats. Mit der Behörde für Inneres besteht Einvernehmen, dass dies durch eine Ergänzung der Ausländerdatenverarbeitungsverordnung erfolgen kann.

17. Verkehrsangelegenheiten

Online-Angebote des Landesbetriebs Verkehr im HamburgGateway

Die E-Government-Angebote des Landesbetriebs Verkehr sind datenschutzgerecht realisiert. Wenn jedoch Medienbrüche durchgehend vermieden werden sollen, müssen zusätzliche technische Sicherheitsmaßnahmen ergriffen werden.

Im Sommer 2005 hat uns der Landesbetrieb Verkehr (LBV) Risikoanalysen und Verfahrensbeschreibungen zu verschiedenen Produkten zur Stellungnahme vorgelegt, die über das HamburgGateway angeboten werden sollen. Für solche neuen Online-Anwendungen müssen vor der Entscheidung über die Einführung Risikoanalysen erstellt werden, in denen die verfahrensspezifischen Bedrohungen und die erforderlichen technischen und organisatorischen Schutzmaßnahmen dargelegt werden. In konstruktiven Gesprächen mit dem LBV wurden datenschutzgerechte und kundenorientierte Lösungen gefunden.

- Sonntagsfahrgenehmigungen

  Mit diesem Service können Firmen, die vom LBV vorab eine entsprechende Berechtigung erhalten haben, Anträge komplett elektronisch stellen. Da die Genehmigungen bei Kontrollen im Original vorgelegt werden müssen, müssen sie noch per Post zugesandt oder von den Antragstellern abgeholt werden.

  Die erforderliche Risikoanalyse wurde erst nach Beginn der Pilotierung erstellt und mit uns erörtert. Im Ergebnis bestanden keine datenschutzrechtlichen Bedenken.

- KFZ-Wunschkennzeichen

  Mit diesem Verfahren soll Großkunden, kleineren Autohändlern und Privaten die Möglichkeit eröffnet werden, sich vor Anmeldung eines KFZ im Rahmen der Verfügbarkeit Wunschkennzeichen reservieren zu lassen. Die fällige Gebühr müssen die Privaten über die integrierte Bezahlschnittstelle des HamburgGateway bezahlen. Die Kennzeichen werden dann für einen Monat im örtlichen Fahrzeugregister reserviert. Da es sich um ein zusätzliches Serviceangebot handelt – die Reservierung ist noch kein Antrag auf Zuteilung des gewünschten Kennzeichens – , ist die Datenverarbeitung nur aufgrund einer Einwilligung der Betroffenen zulässig. Wir haben hierfür nach den Adressatengruppen differenzierte Einwilligungserklärungen vorgeschlagen. Bei Privaten soll zur Identifizierung der Reservierung auch ein Pseudonym reichen. Wir haben deshalb gebeten, hierauf im Dialog auch hinzuweisen.

- Führerschein-Erstantrag

  Das Verfahren sieht vor, den erstmaligen Antrag auf Erteilung einer Fahrerlaubnis in elektronischer Form entweder selbst oder über die ausbildende

Fahrschule stellen zu können. Alle dafür erforderlichen Unterlagen sollen auf dem Postweg nachgereicht werden. Dies gilt wegen der gesetzlich vorgeschriebenen Schriftform (vgl. § 21 Abs. 1 der Fahrerlaubnisverordnung) insbesondere für den Antrag, aber auch für ärztliche Gutachten wegen der darin enthaltenen besonders sensiblen Daten. Ohne Medienbruch wäre für den Antrag gemäß § 3 Abs. 2 des Hamburgischen Verwaltungsverfahrensgesetzes eine qualifizierte elektronische Signatur erforderlich. Medizinische Daten könnten nur verarbeitet werden, wenn zusätzliche technische Sicherheitsmaßnahmen ergriffen würden.

- Halterauskunft für die Polizei Hamburg

  Mit diesem Verfahren sollen die hamburgischen Polizeidienststellen automatisierte Abfragen aus dem örtlichen Fahrzeugregister durchführen können. Wir haben darauf bestanden, dass sensible Daten bei der Anfrage durch die Polizeidienststellen nicht verarbeitet werden, die Anfrage aber zur Verhinderung von Missbräuchen nachvollziehbar bleibt und entsprechend protokolliert wird.

DATENSCHUTZ IM NICHT-ÖFFENTLICHEN BEREICH

18. Internationaler Datenverkehr

18.1 Weitere Entwicklung

Durch die weltweite Vernetzung wird es immer leichter, personenbezogene Daten in andere Länder zu übermitteln, und immer schwerer, den Schutz dieser Daten nach unseren nationalen und europäischen Regelungen tatsächlich zu gewährleisten.

Mit der Erweiterung der Europäischen Union um 10 Länder am 1. Mai 2004 wurde der freie Datenverkehr ausgedehnt. Auch für diese Länder gelten jetzt neben den materiellen Vorschriften des Bundesdatenschutzgesetzes keine weiteren Einschränkungen für die Datenübermittlung (Einzelheiten 19. TB, 18.2).

Zur Vereinfachung von Übermittlungen in Länder außerhalb der EU, die kein angemessenes Datenschutzniveau garantieren, hat die EU-Kommission neben den bereits existierenden Standardvertragsklauseln alternative Standardvertragsklauseln verabschiedet, die seit dem 1. April 2005 einsetzbar sind.

Sofern sich insbesondere internationale Unternehmen für die Einführung verbindlicher Unternehmensregelungen entscheiden, um ausreichende Garantien für die Übermittlung personenbezogener Daten in Drittländer zu schaffen,

ist dies europaweit zu koordinieren. Im Rahmen internationaler Gespräche haben sich die jeweiligen Datenschutzaufsichtsbehörden darauf verständigt, dass die Beurteilung in der Regel von der für den europäischen Hauptsitz zuständigen Aufsichtsbehörde vorgenommen wird. Von ihr werden die Stellungnahmen weiterer beteiligter Aufsichtsbehörden eingeholt.

18.2 Datenübermittlungen in die USA

Die Antiterrorgesetzgebung der USA hat dazu geführt, dass die datenschutzrechtlichen Probleme nur noch auf internationaler Ebene lösbar erscheinen.

Übermittlungen personenbezogener Daten in die USA sind nach dem Bundesdatenschutzgesetz unter verschiedenen Voraussetzungen zulässig. Beispiele dafür sind Banküberweisungen, Reise- oder Hotelverträge, Einwilligungserklärungen, der Beitritt des Daten empfangenden Unternehmens zu den Safe-Harbor-Regelungen, die von der EU-Kommission angemessenes Datenschutzniveau zugesprochen bekommen haben, oder auch die Verwendung von Standardvertragsklauseln.

Obwohl zumindest in den beiden letztgenannten Beispielen ein gewisser – dem deutschen bzw. europäischen Datenschutzrecht vergleichbarer – Mindeststandard gewährleistet werden soll, sind nach deutschen Maßstäben unberechtigte Zugriffe auf personenbezogene Daten nicht ausgeschlossen. Der nach den Anschlägen vom 11. September 2001 in Kraft getretene Patriot Act erlaubt den US-Behörden außerordentlich weit gehende Zugriffsrechte, die durch deutsche Aufsichtsbehörden nicht verhindert werden können. Belegt wird dies durch Beschwerden deutscher Touristen auch bei der hamburgischen Datenschutzaufsichtsbehörde. Bei der Einreise in die USA wurden aus Deutschland kommende Personen damit konfrontiert, dass die Behörden Kenntnisse z. B. über deren Buchbestellungen im Internet hatten.

Die Antiterrorgesetzgebung ist auch verantwortlich für die Forderung der US-Behörden nach der Übermittlung von Flugpassagierdaten durch Fluggesellschaften. Die Fluggesellschaften sehen sich seit März 2003 gezwungen, den Forderungen zu entsprechen, um ihre Landerechte auf US-Flughäfen nicht zu verlieren. Angesichts der Unzulässigkeit dieser Übermittlungen aus europäischer Sicht fanden etliche Gespräche zwischen der EU-Kommission und den US-Behörden statt. Im Ergebnis traf die EU-Kommission trotz massiver Bedenken im Mai 2004 eine sog. Angemessenheitsentscheidung nach Art. 25 Abs. 6 der Europäischen Datenschutzrichtlinie. Noch nicht entschieden ist über die Klage des Europäischen Parlaments vor dem Europäischen Gerichtshof gegen ein bilaterales Abkommen, das die rechtliche Grundlage für die Übermittlungen darstellen soll.

Festzuhalten ist, dass die personenbezogenen Daten eines jeden Flugpassagiers an die US-Behörden übermittelt werden.

19. Tele- und Mediendienste

19.1 Neuregelung des Telemedienrechts

Nachdem die Arbeiten an dem Entwurf eines Telemediengesetzes des Bundes Anfang bis Mitte 2005 deutlich intensiviert worden waren, ist jetzt wieder offen, wann und mit welchem Inhalt das Gesetz verabschiedet wird.

Die geltenden Vorschriften des Teledienstegesetzes, des Teledienstedatenschutzgesetzes und des Mediendienste-Staatsvertrages sollen durch ein einheitliches Telemediengesetz (TMG) des Bundes ersetzt werden. Die 2003 ins Stocken geratenen Arbeiten an einem Gesetz zur Vereinheitlichung des elektronischen Geschäftsverkehrs (vgl. 19. TB, 3.11) wurden Anfang 2005 mit klaren Zeit- und Zielvorgaben wieder aufgenommen. Zunächst in Aussicht genommene Änderungen der Rechtslage wurden nicht mehr weiter verfolgt. Vielmehr wurde ein Gesetzentwurf erarbeitet, dessen materielle Datenschutzbestimmungen sehr weit gehend dem geltenden Recht entsprechen. Insbesondere ist eine grundsätzliche Veränderung der Aufsichtsstruktur, über die noch 2 Jahre zuvor debattiert wurde, in dem neuen Entwurf nicht mehr enthalten.

19.2 Spiel oder Überwachung

Neue technische Möglichkeiten führen immer wieder zur Entwicklung von Produkten, die den Schutz der Privatsphäre außer Acht lassen.

Anfang 2005 erhielten wir Kenntnis von dem Vorhaben eines Internetanbieters, ein neues Produkt auf den Markt zu bringen. Ziel des Produkts war es, dem Nutzer über das Internet anzuzeigen, wo sich eine Person, die ein Handy in Betrieb hat, gerade befindet. Dies sollte über die Ortung des Handys der anderen Person und über eine Anzeige des Standorts auf einem Stadtplan bzw. einer Landkarte im Internet erfolgen. Um den Dienst datenschutzgerecht nutzen zu können, hätte die dritte Person ihre ausdrückliche Zustimmung zur Ortung durch Angabe ihrer Handynummer auf einem Formular im Internet geben müssen. In erster Linie sollte der Dienst mit Einwilligung des Handyinhabers erfolgen, die durch ein aufwändiges Verfahren sichergestellt werden sollte.

Zweifel hinsichtlich der Einwilligung haben sich jedoch bei der Frage ergeben, ob der Teilnehmer seine Einwilligung bewusst und eindeutig erklärt hat. Andererseits blieb unklar, ob der Geortete auch tatsächlich von dem einzelnen Ortungsvorgang Kenntnis erlangen sollte. Durch die in Aussicht genommene besondere Möglichkeit, über ein Handy per SMS die Einwilligung erklären zu können, hätten sich erhebliche Missbrauchsmöglichkeiten ergeben. Allein zwei Varianten drängen sich in diesem Zusammenhang auf: Jemand kann das Handy einer anderen Person an sich nehmen und benutzen, um den Dienst heimlich zu installieren. Ferner ist es denkbar, dass eine berechtigte Person den Dienst für sich als Nutzer der Ortungsmöglichkeit installiert, das Handy

dann aber zur Nutzung und im schlimmsten Fall auch zur Überwachung an eine andere Person weitergibt.

Seitens der Datenschutzaufsichtsbehörde wurde daher gefordert, dass ein höherer Sicherheitsgrad hinsichtlich der Einwilligung des tatsächlichen Teilnehmers oder Nutzers gewährleistet sein muss. Da dieser Dienst innerhalb des angebotenen Teledienstes in nicht unerheblichem Umfang Telekommunikationsleistungen enthält und darüber hinaus bundesweite Bedeutung hätte, wurde die Angelegenheit in Zusammenwirken mit dem Bundesbeauftragten für den Datenschutz in einer bundesweiten Arbeitsgruppe der Datenschutzaufsichtsbehörden erörtert. Im Ergebnis wurde von der Mehrheit der Aufsichtsbehörden gefordert, dass vor jedem Ortungsvorgang eine SMS an den zu Ortenden zu übersenden ist. Darüber hinaus wurde eine gelegentliche, zufallsgesteuerte Information, dass der Ortungsdienst aktiv ist, verlangt. Nur so hätte sichergestellt werden können, dass niemand heimlich überwacht wird.

Der Internetanbieter hat bisher auf die Einführung des Produkts verzichtet.

19.3 Webcams an öffentlichen Internetstationen

Die Übertragung von Bildern in das Internet ist nur in sehr begrenztem Umfang zulässig.

Durch eine Presseveröffentlichung wurde der Hamburgische Datenschutzbeauftragte darauf aufmerksam, dass in kostenlos zu nutzenden Internetstationen in zahlreichen Gaststätten oder an anderen öffentlich zugänglichen Orten Webcams installiert waren. Diese Kameras ermöglichten rund um die Uhr Einsicht in ihre Umgebung. Die dabei entstehenden Bilder, die auch Aufnahmen von deutlich erkennbaren Personen enthielten, wurden während der Laufzeit der Kameras ununterbrochen in das Internet eingestellt. Diese Vorgehensweise widersprach eindeutig den datenschutzrechtlichen Vorschriften. Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen ist nur unter genau festgelegten und eng umgrenzten Voraussetzungen zulässig, die hier nicht vorlagen, so dass Aufnahmen von Personen nur mit deren ausdrücklicher Einwilligung hätten erfolgen dürfen.

Erfreulicherweise waren die Kameras schon zu Beginn der Gespräche zwischen dem Unternehmen und der Datenschutzaufsichtsbehörde nicht mehr in Betrieb. Kurze Zeit später erreichte uns die Mitteilung, dass die Live-Videoübertragung endgültig abgestellt wurde. Die Webcam-Funktion kann nur noch zur Fertigung von Standbildern genutzt werden, die dann per E-Mail verschickt werden können.

20. Versicherungswirtschaft

20.1 Einwilligungsklausel in Antragsformularen für Versicherungsverträge

Mit der Versicherungswirtschaft werden Verhandlungen über eine Neufassung der Einwilligungserklärung geführt, die als Bestandteil jedes Versicherungsvertrages von den Antragstellern vor Vertragsabschluss zu unterzeichnen ist. Ziel ist eine datenschutzkonforme, für die Versicherungsnehmer transparentere Klausel.

Der Düsseldorfer Kreis, der Zusammenschluss der Obersten Datenschutzaufsichtsbehörden zur Kontrolle des Datenschutzes in der Privatwirtschaft, hatte in seiner Sitzung im November 2004 die Arbeitsgruppe Versicherungswirtschaft beauftragt, den Umfang der notwendigen Änderung der Einwilligungsklausel in der Versicherungswirtschaft (auch hinsichtlich der zentralen Hinweis- und Warndateien) insbesondere im Hinblick auf die Novellierung des Bundesdatenschutzgesetzes zu prüfen. Anlass für die Befassung des Düsseldorfer Kreises mit dieser Problematik war ein Rechtsgutachten zur Beurteilung der Datenweitergabeklausel in Antragsformularen der Versicherungswirtschaft im Geschäft mit Verbrauchern in Deutschland von Professor Dr. Schwintowski, das im Auftrag der Verbraucher-Zentrale Bundesverband e.V. erstellt wurde. Das Gutachten kommt unter anderem zu dem Ergebnis, dass die von der Versicherungswirtschaft seit 1994 verwendete Einwilligungsklausel, die seinerzeit mit dem Düsseldorfer Kreis und dem Bundesaufsichtsamt für das Versicherungswesen abgestimmt worden war, datenschutzrechtlich unwirksam sei, weil es an einer wirksamen Einwilligung im Sinne des § 4 a BDSG fehle.

Unter dem Vorsitz des Hamburgischen Datenschutzbeauftragten hat die Arbeitsgruppe Versicherungswirtschaft im Berichtszeitraum mehrere Gespräche mit den Vertretern der Versicherungswirtschaft über eine Überarbeitung der Einwilligungsklausel geführt. Ziel ist es, eine für die betroffenen Versicherungsnehmer transparentere Klausel zu erarbeiten und ein Verfahren zu finden, bei dem die Interessen der Betroffenen mehr Berücksichtigung finden als im bisherigen Verfahren.

Aus Sicht der Datenschutzaufsichtsbehörden wird die Gesamtstruktur der bisherigen Klausel, die für die verschiedenen Vertragstypen eine einheitliche Einwilligungsklausel und ein einheitliches Merkblatt vorsieht, den Anforderungen des Datenschutzes nicht gerecht. Da die derzeitige Einwilligungsklausel für eine Vielzahl von unterschiedlichen Versicherungsverträgen genutzt wird, ist sie zu allgemein formuliert und berücksichtigt branchenspezifische Besonderheiten nicht. Dadurch ist die Klausel konturenlos und für die Betroffenen nicht verständlich, was Eingaben an die Datenschutzaufsichtsbehörden immer wieder zeigen. Für die Betroffenen ist der Umfang der Datenverarbeitung auch

unter Berücksichtigung der Erklärungen im Merkblatt nicht erkennbar. Das Merkblatt enthält Informationen über sämtliche infrage kommenden Datenverarbeitungsmöglichkeiten sowie alle in der Versicherungswirtschaft bestehenden Warn- und Hinweissysteme. Nur ein Teil dieser Informationen ist für den jeweiligen Versicherungsvertrag relevant. Es bleibt dem Betroffenen selbst überlassen, sich die Informationen herauszusuchen, die für seinen Vertragstyp zutreffen könnten. Durch die Vielzahl der nicht auf den jeweiligen Vertragstyp abgestimmten Informationen werden die Betroffenen nicht klar über den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung ihrer Daten für ihr Vertragsverhältnis informiert. Die Datenschutzaufsichtsbehörden halten es außerdem als Bedingung für eine wirksame Einwilligungserklärung für erforderlich, dass das Merkblatt vor Abschluss des Vertrages an den Antragsteller ausgehändigt wird, damit sichergestellt ist, dass der Antragsteller vor Unterzeichnung des Antrags Kenntnis von den Datenverarbeitungsvorgängen, in die er einwilligen soll, hat. Zu den einzelnen Einwilligungstatbeständen der Klausel fordern die Datenschutzaufsichtsbehörden eine klarere unmissverständliche Formulierung, damit die Antragsteller sich der wirklichen Sachlage bewusst werden und übersehen können, auf welche Daten sich ihre Einwilligung erstreckt, welche Daten von wem gespeichert werden und an wen diese übermittelt werden dürfen. Insbesondere die Datenweitergabe und -nutzung im Rahmen der Warn- und Hinweissysteme sei in der bisherigen Klausel nur unzureichend dargestellt und für die Antragsteller nicht verständlich. Auch hinsichtlich der weiteren Einwilligungssachverhalte, wie der Datenübermittlung an Rückversicherer, der Datenweitergabe unabhängig vom Zustandekommen des Vertrages und bei anderweitig beantragten und künftigen Verträgen, besteht aus Sicht der Datenschutzaufsichtsbehörden noch Klärungsbedarf über deren Bedeutung und Notwendigkeit.

Die Versicherungswirtschaft teilt die Auffassung der Datenschutzaufsichtsbehörden nicht. Sie hält die Einwilligungserklärung im Zusammenhang mit dem Merkblatt für verständlich. Sowohl die Klausel als auch das Merkblatt habe sich in der Praxis bewährt und zur Rechtssicherheit beigetragen. Die Struktur der Datenschutzklausel sei praxiskonform und interessengerecht. Es liege in der Natur von Massenverträgen, dass diese allgemeingültige vertragliche Klauseln enthalten und auch zusätzliche Merkblätter niemals jeden denkbaren Einzelfall bis ins letzte Detail aufzeigen könnten. Hinsichtlich der Aushändigung des Merkblatts weist die Versicherungswirtschaft darauf hin, dass die Antragsteller nach der Klausel die Möglichkeit hätten, sich das Merkblatt auf Wunsch sofort, d.h. bei Antragstellung vorlegen zu lassen. Diese Praxis stelle sicher, dass die Antragsteller im Zeitpunkt der Einwilligung über die Bedeutung der Einwilligung informiert würden. Die Einwilligungssachverhalte seien interessenkonform, hinreichend erläutert und aus Sicht der Versicherungswirtschaft erforderlich für die zulässige Erhebung, Verarbeitung und Nutzung von perso-

nenbezogenen Daten. Die Auffassung der Versicherungswirtschaft werde durch ein Rechtsgutachten zur Beurteilung der Datenweitergabeklausel in Antragsformularen der deutschen Versicherungswirtschaft von Prof. Dr. Hoeren gestützt, nach der die derzeitige Einwilligungserklärung datenschutzkonform ist.

Die Versicherungswirtschaft ist trotz ihrer rechtlich unterschiedlichen Bewertung zur Überarbeitung der Einwilligungsklausel und des Merkblatts im Konsens mit den Datenschutzaufsichtsbehörden bereit. Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) legte im September 2005 einen ersten Entwurf für eine neue Einwilligungsklausel sowie für je einen Entwurf für ein Merkblatt für den Bereich der Personenversicherung und der Schadenversicherung vor. Grundidee sei eine Einwilligungserklärung mit verständlichen und ausreichenden Informationen. Die ergänzenden Ausführungen im jeweiligen Merkblatt sollten lediglich deklaratorische Wirkung entfalten.

Die Datenschutzaufsichtsbehörden begrüßen grundsätzlich die Bereitschaft der Versicherungswirtschaft zur Überarbeitung der Klausel. Die einzelnen Formulierungen des Entwurfes und der darin vorgesehene Umfang des Datenaustausches stoßen aber mehrheitlich auf Kritik. Trotz der zum Teil verbesserten Verständlichkeit der Klausel bewerten die Datenschutzaufsichtsbehörden den Entwurf insbesondere im Hinblick auf den Umfang der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten im Rahmen der Warn- und Hinweissysteme als nicht ausreichend. Außerdem enthalten sowohl der Entwurf für die Einwilligungsklausel als auch die Merkblätter nach Auffassung der Datenschutzaufsichtsbehörden weiterhin Informationen, die für den konkreten Vertrag nicht relevant sind. Dieses Zuviel an Informationen bei gleichzeitig bestehender Unschärfe der Formulierungen ist für die Versicherungsnehmer irreführend. Als sehr bedenklich bewerten die Datenschutzaufsichtsbehörden die von der Versicherungswirtschaft in dem Entwurf vorgesehene Erweiterung der Allfinanzklausel und die beabsichtigte Einholung einer Einwilligung der Versicherungsnehmer in einen umfassenden Datenaustausch zwischen Versicherungen und Auskunfteien.

In seiner Sitzung im November 2005 hat der Düsseldorfer Kreis sich für eine Fortführung der Gespräche mit der Versicherungswirtschaft ausgesprochen. Der Düsseldorfer Kreis hält deutliche Verbesserungen des von dem GDV vorgelegten Entwurfs der Klausel unter Berücksichtigung der Kritikpunkte der Datenschutzaufsichtsbehörden für erforderlich. Die Mehrheit der Datenschutzaufsichtsbehörden ist weiterhin grundsätzlich bereit, bis zum Abschluss der Gespräche keine aufsichtsbehördlichen Maßnahmen bezüglich der Klausel vorzunehmen. Über den Fortgang der Verhandlungen mit dem GDV werden wir berichten.

20.2 Schweigepflicht-Entbindungserklärung bei Krankenversicherungsanträgen

Zwischen den Obersten Datenschutzaufsichtsbehörden und der Versicherungswirtschaft konnte keine Einigung über eine Änderung der Schweigepflicht-Entbindungserklärung für Leistungsanträge erzielt werden.

Trotz intensiver Erörterungen in der Arbeitsgruppe Versicherungswirtschaft unter dem Vorsitz des Hamburgischen Datenschutzbeauftragten konnte mit der Versicherungswirtschaft keine Einigung auf ein geändertes Verfahren bei der Einholung von Schweigepflicht-Entbindungserklärungen bei Leistungsanträgen in der privaten Krankenversicherung erzielt werden. Die Obersten Datenschutzaufsichtsbehörden haben mehrheitlich erhebliche datenschutzrechtliche Bedenken dagegen, dass bereits bei Abschluss des Versicherungsvertrags eine Schweigepflicht-Entbindungserklärung für alle künftigen Leistungsanträge eingeholt wird, da die Erklärung sich nicht auf konkrete Gesundheitsdaten bezieht. Sie hatten von der Versicherungswirtschaft daher gefordert, dass die Versicherungsunternehmen sich bei jeder Leistungsprüfung eine konkrete auf den Einzelfall bezogene Schweigepflicht-Entbindungserklärung erteilen lassen (vgl. 19. TB Ziffer, 19.1). Die Versicherungswirtschaft ist nicht bereit, das Verfahren zu ändern und im Zusammenhang mit Erstattungsanträgen eine Erklärung einzuholen. Unter Berufung auf ein von der Versicherungswirtschaft eingeholtes Rechtsgutachten von Prof. Sieber, der die gegenwärtige Erklärung für zulässig erachtet, hat sie insbesondere auf einen mit der Umstellung des Verfahrens deutlich erhöhten Verwaltungs- und Kostenaufwand und eine verzögerte Leistungssachbearbeitung hingewiesen.

Die Datenschutzaufsichtsbehörden haben es abgelehnt, sich mit einem von der Versicherungswirtschaft vorgelegten Neuentwurf für Absatz 2 der Schweigepflicht-Entbindungserklärung zu befassen, weil dieser nur eine sprachliche Änderung enthielt, das beanstandete Verfahren aber beibehalten werden sollte. Die Gespräche wurden daher nicht fortgeführt.

Sowohl die Bundesärztekammer als auch die Bundeszahnärztekammer sind von uns über den Abbruch der Verhandlungen unterrichtet worden.

20.3 Warn- und Hinweissysteme

Der Umfang des Datenaustausches im Rahmen der Warn- und Hinweissysteme und deren rechtliche Einordnung ist Gegenstand von Erörterungen in der Arbeitsgruppe Versicherungswirtschaft.

Die zentralen Warn- und Hinweissysteme der Versicherungswirtschaft waren aufgrund ihrer Vielzahl und der sich im Zusammenhang mit der Datenweitergabe ergebenden Problematik immer wieder Gegenstand kritischer Berichterstattung. In den Warn- und Hinweissystemen der verschiedenen Versicherungssparten werden personenbezogene Daten von Versicherungsnehmern

zwischen einzelnen Versicherungsunternehmen ausgetauscht. Der Gesamtverband der Versicherungswirtschaft (GDV) führt keine zentrale Datei mit personenbezogenen Daten. Den Ablauf des Verfahrens zum Datenaustausch haben wir zuletzt im 19. TB, 19.2 beschrieben.

Die rechtliche Bewertung der Warn- und Hinweissysteme sowie der Datenübermittlung durch die Versicherungsunternehmen wird derzeit in der Arbeitsgruppe Versicherungswirtschaft im Zusammenhang mit der Überarbeitung der Einwilligungsklausel in den Antragsformularen für Versicherungsabschlüsse (20.1) erörtert. Auf Wunsch der Datenschutzaufsichtsbehörden hat die Versicherungswirtschaft das System vorgeführt und ausführlich erläutert. Anlass für die erneute Diskussion sind neben der fehlenden Transparenz des gesamten Verfahrens insbesondere Bedenken der Datenschutzaufsichtsbehörden gegen die Weitergabe aller codierten Daten an sämtliche Versicherungsunternehmen einer Branche, obwohl diese nur ein berechtigtes Interesse an einzelnen Datensätzen haben.

Darüber hinaus sind die Kriterien für eine Meldung von personenbezogenen Daten in die Warn- und Hinweissysteme wieder Gegenstand eingehender Diskussionen mit dem GDV. Dabei geht es insbesondere um die Voraussetzungen, unter denen personenbezogene Daten in das Warn- und Hinweissystem der Rechtsschutzversicherer eingemeldet werden können. Diese Voraussetzungen waren zuletzt 1993 festgesetzt worden. Grund für die erneute Diskussion sind Hinweise darauf, dass einige Versicherungen bereits die Anfrage eines Versicherten, ob Rechtsschutz in einem von ihm geschilderten Fall bestehen könnte, als Versicherungsfall werten, auch wenn es tatsächlich nicht zu einem Verfahren kommt. Würde diese Annahme zutreffen, wäre nach den 1993 festgelegten Meldekriterien eine Einmeldung in das Warn- und Hinweissystem der Rechtsschutzversicherer grundsätzlich bereits möglich, wenn ein Versicherungsnehmer zweimal innerhalb eines Jahres bei seiner Versicherung eine entsprechende Anfrage stellt und er daraufhin gekündigt wird. Eine solche Risikobewertung wäre mit den schutzwürdigen Interessen der Versicherungsnehmer nicht zu vereinbaren. Die Versicherungswirtschaft tritt dieser Darstellung entgegen und hat sich bereit erklärt, die Sachlage aufzuklären.

Von der Arbeitsgruppe Versicherungswirtschaft wird erneut die Frage der Benachrichtigung von in den Warn- und Hinweissystemen gespeicherten Beteiligten, z. B. Zeugen und Geschädigten, die nicht Versicherungsnehmer sind, thematisiert. Die Zulässigkeit der Speicherung und Übermittlung der Daten von Beteiligten richtet sich nach § 28 Abs. 2 und Abs. 3 BDSG. Danach sind die schutzwürdigen Interessen der jeweils Betroffenen an dem Ausschluss der Speicherung oder Übermittlung und die berechtigten Interessen der Versicherungswirtschaft an der Verhinderung und Aufklärung von Fällen des Versicherungsbetruges gegeneinander abzuwägen. Ein Betroffener, der keine Kenntnis von einer Speicherung und Übermittlung seiner Daten erlangt, hat nicht die

Möglichkeit, seine schutzwürdigen Interessen zu vertreten. Im Jahr 1991 wurde mit der Versicherungswirtschaft vereinbart, dass die Betroffenen über die Speicherung ihrer Daten und deren mögliche Weitergabe im Rahmen der Warn- und Hinweissysteme unterrichtet werden. Aus Beschwerden an die Datenschutzaufsichtsbehörden geht hervor, dass sich einige Versicherungen nicht an diese Vereinbarung halten.

20.4 Datenaustausch zwischen Versicherungen und Auskunfteien

Der von der Versicherungswirtschaft angestrebte umfangreiche Datenaustausch zwischen Versicherungsunternehmen und Auskunfteien stößt auf erhebliche Bedenken.

Die Datenschutzaufsichtsbehörden haben erhebliche Bedenken gegen die Einholung von Bonitätsauskünften durch Versicherungsunternehmen bei Auskunfteien im Zusammenhang mit dem Abschluss oder der Durchführung von Versicherungsverträgen, da sie diesen Datenaustausch nicht für erforderlich halten.

Im Zusammenhang mit der Überarbeitung der Einwilligungsklausel hat die Versicherungswirtschaft in ihren Entwurf für eine neue Klausel eine Einwilligungserklärung der Versicherungsnehmer eingefügt, die die Einholung von Auskünften von Auskunfteien bei Vertragsschluss, im Rahmen der Vertragsabwicklung sowie bei Zahlungsverzug einschließlich der Einholung eines Scorewertes erlauben soll. Die Datenschutzaufsichtsbehörden haben demgegenüber auf ihre eindeutige ablehnende Beschlusslage hingewiesen. Danach ist die Einholung einer Bonitätsauskunft bei Abschluss einer Versicherung nicht erforderlich, da das Versicherungsunternehmen von der Leistung befreit ist, wenn die Prämien nicht bezahlt werden. Bisher ist von der Versicherungswirtschaft nicht nachvollziehbar dargelegt worden, aus welchem Grund die Versicherungen Auskünfte bei Auskunfteien einholen wollen. Zu berücksichtigen ist dabei, dass die Versicherungswirtschaft bereits jetzt über einen umfangreichen Datenbestand und gute Möglichkeiten zur Risikoabwägung infolge der branchenspezifischen Warn- und Hinweissysteme verfügt. Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) wurde gebeten, das berechtigte Interesse der Versicherungswirtschaft an einem Datenaustausch mit Auskunfteien darzulegen.

20.5 EU-weite Prüfung der Datenverarbeitung durch Krankenversicherungen

Im Interesse einer einheitlichen Durchsetzung der Datenschutzbestimmungen erfolgt eine koordinierte Fragebogenaktion in den Mitgliedstaaten zur Datenverarbeitung durch private Krankenversicherungen.

Die Art. 29 Datenschutzgruppe beabsichtigt unionsweit abgestimmte Durchsetzungsmaßnahmen der EU-Mitgliedsstaaten mit dem Ziel einer aktiveren

Anwendung und Überwachung des Datenschutzrechts in der EU. Aus Sicht der Gruppe sind dafür zunächst koordinierte Prüfungen in den Mitgliedstaaten erforderlich, die vergleichbare Verarbeitungen der EU-Länder im Visier haben und sich auf Fragenkataloge stützen, die auf Unionsebene vereinbart worden sind. Dabei soll geklärt werden, ob die Verarbeitungen mit dem nationalen und dem EU-Recht vereinbar sind. Anschließend sollen – falls erforderlich – Maßnahmen zur Rechtsdurchsetzung auf EU-Ebene erörtert werden.

Im April 2005 hat die Art. 29 Datenschutzgruppe auf Vorschlag der spanischen und niederländischen Aufsichtsbehörde beschlossen, den privaten Krankenversicherungsbereich auf die Einhaltung des Datenschutzes hin zu überprüfen. Die spanische Aufsichtsbehörde hat dazu einen Fragebogen entworfen. Am 8. November 2005 fand dazu in Brüssel eine Sitzung der Enforcement Arbeitsgruppe statt. An dieser Sitzung nahmen Mitglieder der CEA, des europäischen Verbandes der nationalen Versicherungsverbände, teil. Die Vertreter informierten über die Struktur, die Besonderheiten und den Leistungsumfang der privaten Krankenversicherungen in den einzelnen Mitgliedsländern. Sie gaben zu bedenken, dass eine Vergleichbarkeit der Datenverarbeitung in den Mitgliedsländern nur schwer möglich sei, da der jeweilige Umfang der Erhebung und Verarbeitung von personenbezogenen Daten im Zusammenhang mit dem Abschluss der Krankenversicherungen in den Mitgliedsländern sehr unterschiedlich sei.

In der Sitzung wurde vereinbart, dass die Versendung der Fragebögen an einzelne Krankenversicherungsunternehmen in den Mitgliedsländern in den ersten drei Monaten des Jahres 2006 erfolgen soll. Kriterien für die Auswahl der zu befragenden Unternehmen sind deren Größe, Marktanteil und Bedeutung. In Deutschland sollen die mindestens 5 zu befragenden Unternehmen nach Rücksprache mit dem Verband der privaten Krankenversicherungen (PKV) ausgewählt werden. Wir werden ein Hamburger Unternehmen in die Prüfung einbeziehen.

Nach Rücklauf der Antworten erfolgt auf nationaler Ebene eine Zusammenfassung der Ergebnisse der Fragebogenaktion. Da Hamburg den Vorsitz in der Arbeitsgruppe Versicherungswirtschaft hat, werden wir die Koordinierung der Aktion und Zusammenfassung der deutschen Ergebnisse übernehmen. Die nationalen Ergebnisse werden dann in einen gemeinschaftlichen Bericht der Mitgliedsländer über die Durchführung der Fragebogenaktion aufgenommen werden. Der Abschlussbericht soll der Art. 29 Gruppe nach dem derzeitigen Zeitplan Ende des Jahres 2006 vorgelegt werden. Über die Durchführung der Aktion werden wir berichten.

21. Schufa

21.1 Datenaustausch mit Inkassounternehmen

Die Schufa entwickelte sich in den letzten Jahren weg von einer Auskunftei für angeschlossene Kreditinstitute hin zu einem umfassenden Auskunftssystem für viele Wirtschaftsbereiche.

Zwar hat die Schufa von dem Vorhaben Abstand genommen, auch an Sicherheitsunternehmen vor der Einstellung neuer Mitarbeiter Auskünfte zu erteilen. Die Teilnahme von Inkassounternehmen am Schufa-Verfahren wird jedoch weiter verfolgt. Dabei sollen Inkassounternehmen nicht nur die Möglichkeit erhalten, Auskünfte bei der Schufa einzuholen, sondern ihrerseits verpflichtet werden, die Forderungen ihrer Kunden – bei denen es sich nicht zwangsläufig um Schufa-Anschlusspartner handelt – unter bestimmten Voraussetzungen einzumelden. Die Datenschutzaufsichtsbehörden haben der Schufa mitgeteilt, dass unter diesen Umständen nur rechtskräftig titulierte Forderungen gemeldet werden dürfen. Die vorläufige Vollstreckbarkeit wird nicht als ausreichend angesehen. Darüber hinaus dürften die Forderungen erst 6 Wochen nach der Titulierung gemeldet werden, um dem Betroffenen ausreichend Zeit zur Zahlung einzuräumen. Mit diesen Voraussetzungen hatte die Schufa sich zunächst einverstanden erklärt. In einem neueren Schreiben ist sie davon jedoch abgerückt und fordert weitergehende Meldemöglichkeiten für Inkassounternehmen. Ein abschließendes Ergebnis konnte noch nicht erzielt werden.

Zu der besonderen Problematik der Erteilung von Auskünften an Versicherungsunternehmen durch die Schufa und andere Auskunfteien siehe 20.4.

21.2 Sicherung der Vertraulichkeit bei Erteilung kostenfreier Selbstauskünften

Die Vertraulichkeit bei der Erteilung von kostenfreien Selbstauskünften in den Schufa-Geschäftsstellen ist nicht gewährleistet.

Bei der Datenschutzaufsichtsbehörde Hamburg, aber auch bei den Aufsichtsbehörden anderer Bundesländer sind im Berichtszeitraum Beschwerden über mangelnde Vertraulichkeit bei der Einholung kostenloser Schufa-Selbstauskünfte eingegangen. Neben der Aushändigung einer kostenpflichtigen Selbstauskunft ist die Schufa gesetzlich verpflichtet, dem Betroffenen auch die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten und Angaben zu verschaffen. Da die Auskunftserteilung vor Ort aber in der Regel in der Weise organisiert war, dass mehrere Auskunft erteilende Schufa-Mitarbeiter in einem Raum sitzen und die Auskunft dem Betroffenen vorgelesen wird, konnten die Betroffenen bisher keine Auskunft erlangen, ohne dass fremde Zuhörer dies mitverfolgen konn-

ten. Dadurch wurden teilweise sensible Tatsachen zwangsläufig Unbeteiligten offenbart.

Nach Kritik an diesem Verfahren ist die Schufa jetzt dazu übergegangen, dem Betroffenen die Selbstauskunft auszuhändigen. Dadurch wird ihm Gelegenheit gegeben, die Unterlagen einschließlich der üblichen Informationen in der Geschäftsstelle selbst durchzulesen. Sollte er anschließend Fragen an die Schufa-Mitarbeiter haben, wird er darauf hingewiesen, dass dieses Gespräch gegebenenfalls von den anderen Kunden mitgehört werden könne und er daher auch die Möglichkeit habe, sich schriftlich mit Fragen an die Schufa zu wenden oder abzuwarten, bis die übrigen Kunden den Raum verlassen haben. Lediglich die Informationsunterlagen, nicht aber die Auskunft selbst – die kostenpflichtig wäre – kann der Betroffene anschließend mitnehmen. Aus Sicht der Datenschutzaufsichtsbehörden ist dieses Vorgehen nicht besonders kundenfreundlich, nach den Vorschriften des Bundesdatenschutzgesetzes jedoch nicht zu beanstanden. Besser wäre es, den Betroffenen die Möglichkeit zu eröffnen, ihre Fragen und Bemerkungen in einem separaten Raum erörtern zu können.

21.3 Altersüberprüfung durch die Schufa bei Internetnutzern

Der sichere Ausschluss Jugendlicher von Internetspielen, die Erwachsenen vorbehalten sein sollen, kann durch ein einfaches Altersüberprüfungsverfahren nicht gewährleistet werden.

Ein Zigarettenhersteller bietet im Internet für verschiedene Zigarettenmarken als Werbemaßnahme Telespiele an. Um Jugendliche von dieser Tabakwerbung auszuschließen, wird vom Spieleanbieter vor dem Zugang zu diesen Spielen eine Altersüberprüfung durch die Schufa vorgenommen. Dafür werden Vorname, Nachname, Adresse sowie das Geburtsdatum abgefragt. Darüber hinaus ist ein Sicherheitscode einzutragen. Gleichzeitig wird darüber informiert, dass die Berechtigung, an den Spielen teilzunehmen, durch Übermittlung der Daten an die Schufa überprüft wird. Die Schufa meldet nach entsprechendem Datenabgleich an den Spieleanbieter ein prozentuales Ergebnis über die Volljährigkeit zurück, nicht jedoch bei ihr gespeicherte Daten.

Diese Verfahrensweise hat angesichts der Tatsache, dass die Erbringung von Telediensten grundsätzlich auch anonym möglich sein muss, die Frage aufgeworfen, wie im Internet sichergestellt werden kann, dass besonderen Zugang nur Berechtigte erhalten können. Das Problem stellt sich für viele Angebote, deren Inhalt zwar nicht als unzulässig anzusehen ist, deren Aufruf aber Altersgrenzen unterliegt. Hierzu zählen unter anderen Angebote aus dem Bereich Pornographie oder Gewaltdarstellungen.

Unabhängig davon, ob im vorliegenden Fall tatsächlich eine gesetzliche Verpflichtung des Teledienstanbieters zur Altersüberprüfung besteht, ist fraglich,

ob mit dieser Maßnahme das Ziel des Ausschlusses jugendlicher Nutzer erreicht werden kann. Es ist wenig lebensnah anzunehmen, dass jugendliche Nutzer, die sich mit den Gepflogenheiten und der relativen Anonymität des Internet meist besser auskennen als Erwachsene, ihre richtigen Daten eingeben. Die Abfrage der Daten scheint wenig geeignet, das Ziel des Ausschlusses von Jugendlichen zu erreichen. Die Datenabfrage würde daher weitgehend ins Leere laufen oder falsche Ergebnisse produzieren.

Wegen der bundesweiten Bedeutung der Angelegenheit wurde das Thema in der AG Telekommunikation, Tele- und Mediendienste des Düsseldorfer Kreises mit den Aufsichtsbehörden der übrigen Bundesländer und einem Vertreter des Bundesdatenschutzbeauftragten diskutiert und Kontakt zur Kommission für Jugendmedienschutz (KJM) hergestellt. Die KJM hat für einen Zugangsschutz für geschlossene Benutzergruppen schon im Jahre 2003 Anforderungen festgelegt. Danach ist der Zugangsschutz durch zwei Schritte sicherzustellen: Erstens durch eine zumindest einmalige zuverlässige Volljährigkeitsprüfung (Identifizierung), die über einen persönlichen Kontakt erfolgen muss, und zweitens durch eine sichere Authentifizierung bei jedem Nutzungsvorgang, um das Risiko der Manipulation, Weitergabe oder des sonstigen Missbrauchs von Zugangsdaten an Minderjährige zu minimieren.

Die AG Telekommunikation, Tele- und Mediendienste des Düsseldorfer Kreises wird mit der KJM Gespräche über die datenschutzrechtlichen Auswirkungen von Altersverifikationsprogrammen führen. In diesem Rahmen wird die Problematik insbesondere im Hinblick auf die Geeignetheit der Programme vertieft werden.

22. Neue Auskunftei-Geschäftsmodelle

Immer wieder versuchen Unternehmen, neue Auskunfteimodelle zu etablieren, die nicht den datenschutzrechtlichen Vorgaben entsprechen.

Im Berichtszeitraum erreichten die Datenschutzaufsichtsbehörde wieder mehrere Hinweise auf Warndateien, die über das Internet Auskünfte über personenbezogene Daten wie das Zahlungsverhalten von Kunden anbieten. Bereits im 19. TB, 21.3 wurden die datenschutzrechtlichen Anforderungen an die Zulässigkeit solcher Verfahren dargestellt. Auch die jetzt bekannt gewordenen Modelle mussten als unzulässig eingestuft werden.

Darüber hinaus hat die Datenschutzaufsichtsbehörde seit Mitte 2005 einen besonders gravierenden Fall zu beurteilen. Der betriebliche Datenschutzbeauftragte eines Unternehmens wandte sich an den Hamburgischen Datenschutzbeauftragten, um im Vorfeld der Einführung einer neuen Auskunftei die datenschutzrechtlichen Anforderungen zu besprechen. Aus den vorgelegten Unterlagen ging hervor, dass neben zulässigen Daten auch pauschal das

Zahlungsverhalten, fällige offene Posten, fällige offene Posten der letzten 30 Tage, Ausschöpfen von Zahlungszielen und Kreditlinien, Zahlungsproteste, Inkassoaufträge, Ratenzahlungen, Mahnbescheide und strittige Verfahren gemeldet und abgefragt werden sollen. Diese Liste war neben anderen datenschutzrechtlichen Mängeln dieses Verfahrens so gravierend, dass der betriebliche Datenschutzbeauftragte sofort darüber informiert wurde, dass es rechtswidrig ist, die genannten personenbezogenen Daten in die Auskunfteitätigkeit aufzunehmen.

Das geschäftsmäßige Erheben und Speichern personenbezogener Daten zum Zwecke der Übermittlung ist nur dann zulässig, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung oder Speicherung hat. Es ist allgemein anerkannt, dass diese Voraussetzung dann nicht vorliegt, wenn es sich nicht eindeutig um ein sog. negatives Merkmal handelt, das die Kreditwürdigkeit des Betroffenen einschränkt. Im 19. TB, 21.1 wurde ausführlich über die Aufnahme von Negativmerkmalen berichtet. Im hier vorgelegten Geschäftsmodell sollen zusätzlich Merkmale eines normalen vertragsgerechten Verhaltens, wie etwa das Ausschöpfen von Zahlungszielen gemeldet und an Interessierte weiter übermittelt werden. Das ist unzulässig.

Dem betrieblichen Datenschutzbeauftragten und einem der Geschäftsführer des Unternehmens wurde in einem Gespräch die Rechtswidrigkeit des Geschäftsmodells verdeutlicht. Dennoch wurde, ohne – wie gesetzlich vorgeschrieben – auch nur eine Registermeldung zu erwirken, kurze Zeit später das beschriebene Geschäftsmodell im Internet angeboten. Die Datenschutzaufsichtsbehörde wird die ihr zur Verfügung stehenden rechtlichen Maßnahmen ergreifen, um die Auskunftei in der vorgesehenen rechtswidrigen Ausgestaltung zu verhindern.

23. Kreditwirtschaft

23.1 Kreditscoring

Bei der Nutzung von Scoring-Verfahren im Zusammenhang mit Bankkrediten fordern die Obersten Datenschutzaufsichtsbehörden mehr Transparenz für die Betroffenen.

Im Zusammenhang mit Basel II, der Eigenkapitalübereinkunft der im Baseler Ausschuss für Bankenaufsicht versammelten europäischen Finanzaufsichtsbehörden und Zentralbanken, gewinnen Scoring-Verfahren eine zunehmende Bedeutung. Die EU-Kommission erarbeitet derzeit eine Richtlinie zur Umsetzung von Basel II. Das Basel II-Abkommen definiert die Mindestanforderungen an die Eigenkapitalausstattung von Kreditinstituten. Daraus ergibt sich mittelbar, dass Kredite künftig nicht mehr pauschal, sondern differenziert nach dem

tatsächlichen Risiko mit Eigenkapital zu unterlegen sind. Kredite mit höherem Ausfallrisiko erfordern eine höhere Eigenkapitalunterlegung. Zur Ermittlung der Eigenkapitalquote ist eine differenzierte Risikoklassifizierung notwendig.

Als ein Verfahren zur Risikoklassifizierung wird das Kreditscoring zur Feststellung und Beurteilung der Kreditwürdigkeit von Antragstellern und zur Bonitätsbewertung während der Laufzeit eines Kredits eingesetzt. Dabei werden die verschiedenen Merkmale eines Antragstellers (z. B. Alter, ausgeübter Beruf, Einkommensklasse, Familienstand, Kinderzahl, Wohndauer, Kfz-Besitz, Anzahl der Kredite), die zum Zeitpunkt der Antragstellung oder während der Laufzeit des Kredites vorliegen, auf ihre Risikorelevanz geprüft. Durch den Vergleich der Merkmalsprofile von Kunden mit guter und schlechter Zahlungshistorie lassen sich so Risikofaktoren erkennen. Das Ergebnis des Vergleichs drückt sich in einem Score-Wert aus, der die statistische Bonitätsbewertung der konkreten Antragsteller in einem Zahlenwert zusammenfasst. Das Kreditscoring und die Festlegung der entsprechenden Parameter kann durch das Kreditinstitut selbst erfolgen oder durch einen Dritten, z. B. eine Auskunftei oder einen sonstigen Dienstleister.

Der Scorewert selbst ist ein personenbezogenes Datum im Sinne des § 3 Abs. 1 BDSG, bei dessen Erhebung, Verarbeitung und Nutzung die datenschutzrechtlichen Vorschriften zu beachten sind. In der Arbeitsgruppe Kreditwirtschaft des Düsseldorfer Kreises erörtern die Obersten Datenschutzaufsichtsbehörden mit Vertretern der Kreditwirtschaft, welche personenbezogenen Daten für das Kreditscoring erhoben, verarbeitet und genutzt werden dürfen und welche Transparenzanforderungen aus Sicht des Datenschutzes an das Kreditscoring zu stellen sind. Nach Auffassung der Obersten Datenschutzaufsichtsbehörden dürfen für das Scoring-Verfahren nur Parameter eingestellt werden, deren Bonitätsrelevanz durch ein mathematisch-statistisches Verfahren, das wissenschaftlichen Standards entspricht, nachgewiesen werden. Es dürfen nach § 28 Abs. 1 Nr. 1 BDSG nur Daten erhoben und gespeichert werden, die zur Zweckbestimmung des Vertragsverhältnisses erforderlich sind. Für die Betroffenen muss transparent sein, welche personenbezogenen Daten grundsätzlich in die Berechnung des Score-Wertes einfließen, welche personenbezogenen Daten des Antragstellers für das Scoring-Verfahren konkret genutzt werden und gegebenenfalls welches die maßgeblichen Merkmale sind, die einen konkreten Score-Wert negativ beeinflusst haben.

Darüber hinaus ist bei der Anwendung eines Scoring-Verfahrens stets § 6a BDSG zu beachten. Unzulässig sind daher Scoring-Verfahren, die Kreditsuchende bei Zuordnung zu einer bestimmten Risikogruppe aufgrund einer automatisierten Einzelentscheidung von der Kreditvergabe ausschließen, ohne dass die Kreditsuchenden die Möglichkeit haben, ihren Standpunkt geltend zu machen und anschließend überprüfen zu lassen.

23.2 Übermittlung von Bankdaten an andere Kreditinstitute

Die Zusammenarbeit von Kreditinstituten führt zu datenschutzrechtlichen Problemen, wenn dabei Kundendaten ohne Einwilligung der Betroffenen weitergegeben werden.

Ein in Hamburg ansässiges Kreditinstitut lässt einige Aufgaben, die im Zusammenhang mit Prolongationen und der Anpassung der Konditionen von Hypothekendarlehensverträgen stehen, aus Rationalisierungsgründen und wegen der dort in besonderem Maße vorhandenen Sachkenntnis durch Mitarbeiter einer Bausparkasse durchführen. Zwischen den Unternehmen wurde ein Vertrag nach § 11 BDSG geschlossen, der vorsieht, dass der beauftragten Bausparkasse regelmäßig die Daten von Kreditnehmern, bei denen eine Anpassung bevorsteht, übermittelt werden. Zu den Aufgaben der beauftragten Bausparkasse gehört neben der Unterstützung bei der Planung der Kundenansprache in Einzelfällen auch die direkte Ansprache der Kreditnehmer.

Es ist zweifelhaft, ob die von dem Kreditinstitut auf die Bausparkasse durch den Vertrag übertragenen Tätigkeiten im Wege einer Auftragsdatenverarbeitung nach § 11 BDSG durchgeführt werden können. Durch den Vertrag wird der Bausparkasse nicht nur die Verarbeitung von personenbezogenen Daten übertragen, sondern es werden auch die Aufgaben übertragen, zu deren Erfüllung die Verarbeitung und Nutzung der Daten erforderlich ist. Nach Auffassung der Obersten Datenschutzaufsichtsbehörden liegt in derartigen Fällen eine Funktionsübertragung vor. Die Weitergabe der Kundendaten an die Bausparkasse wird als Übermittlung im Sinne des § 3 Abs. 4 Nr. 3 BDSG angesehen, für deren Zulässigkeit eine Rechtsgrundlage erforderlich ist. § 28 Abs. 1 Nr. 1 BDSG kommt als Rechtsgrundlage nicht in Betracht, da die Auslagerung einer Betreuungstätigkeit nicht unmittelbar der Zweckbestimmung des Darlehensvertrages dient. Die Datenübermittlung und Nutzung durch die Bausparkasse ist auch nicht nach § 28 Abs. 1 Nr. 2 BDSG zulässig, da aufgrund des Bankgeheimnisses die schutzwürdigen Interessen der Darlehensnehmer an einem Ausschluss der Weitergabe ihrer personenbezogenen Daten überwiegen. Nach Auffassung der Datenschutzaufsichtsbehörden ist die mit der Funktionsübertragung verbundene Übermittlung von personenbezogenen Kundendaten an die Bausparkasse nur mit Einwilligung der Kunden datenschutzrechtlich zulässig. Das Kreditinstitut und die Bausparkasse teilen diese Auffassung nicht.

Nicht nur in diesem Einzelfall gibt es zwischen den Vertretern der Wirtschaft und der Obersten Datenschutzaufsichtsbehörden unterschiedliche Rechtsauffassungen dazu, wann eine Auftragsdatenverarbeitung nach § 11 BDSG und wann eine Funktionsübertragung vorliegt. Während die Vertreter der Wirtschaft den Begriff der Auftragsdatenverarbeitung sehr weit auslegen und Unterstützungsdienstleistungen grundsätzlich als Auftragsdatenverarbeitung ausgestalten möchten, sind die Obersten Datenschutzaufsichtsbehörden der Auffassung, dass in jedem Einzelfall der Umfang der Verlagerung der Aufga-

ben bei der Abgrenzung betrachtet werden muss. Im Bereich der Kreditwirtschaft ist außerdem die Beachtung des Bankgeheimnisses von besonderer Bedeutung. Liegt keine Auftragsdatenverarbeitung vor, ist eine datenschutzrechtlich zulässige Realisierung einer Aufgabenverlagerung und der damit verbundenen Datenübermittlung im Wege der Funktionsübertragung nur möglich, wenn die Zulässigkeitsvoraussetzungen durch besondere Maßnahmen wie die Einholung einer Einwilligung der Kunden oder die Vertragsgestaltung geschaffen werden.

23.3 Schufa-Klausel bei Guthabenkonten / Konto für Jedermann

Wird bei Beantragung eines Guthabenkontos zunächst von den Banken die Eröffnung eines gewöhnlichen Girokontos geprüft, besteht hinsichtlich der Prüfung dieses Girokontos ein berechtigtes Interesse an einer Schufa-Abfrage.

Die Frage, ob vor der Eröffnung eines Girokontos auf Guthabenbasis die Unterzeichnung einer Schufa-Klausel von den Banken verlangt werden kann, war auch im Berichtszeitraum Gegenstand von Erörterungen zwischen den Obersten Datenschutzaufsichtsbehörden und Vertretern des Zentralen Kreditausschusses (ZKA). Zuletzt hatten wir darüber im 19. TB, 22.1 berichtet. Von Seiten der Kreditwirtschaft wurde darauf hingewiesen, dass es bei den Banken kein eigenständiges Produkt „Guthabenkonto“ gebe. Die Selbstverpflichtung der Banken aus dem Jahr 1995 beziehe sich daher nicht auf die Eröffnung eines „Guthabenkontos“, sondern auf die Eröffnung eines Girokontos in der Modalität eines Guthabenkontos. Selbst bei ausdrücklicher Beantragung eines Guthabenkontos würde zunächst immer die Eröffnung eines Girokontos mit Überziehungsmöglichkeit geprüft. Hinsichtlich der Prüfung eines Kontos mit Überziehungsmöglichkeit besteht nach Auffassung der Obersten Datenschutzaufsichtsbehörden ein berechtigtes Interesse der Banken gem. § 29 Abs. 2 Ziffer 1a BDSG, eine Schufa-Auskunft einzuholen.

Unabhängig von der datenschutzrechtlichen Problematik ist die Umsetzung der vom ZKA ausgesprochenen Selbstverpflichtung zum „Girokonto für Jedermann“ durch die Banken weiterhin, insbesondere bei den Schuldnerberatungsstellen, umstritten.

24. Werbung

24.1 Telefonwerbung für die Nordwestdeutsche Klassenlotterie

Lose am Telefon verkaufen: Aber bitte nur mit Einwilligung!

Im Berichtszeitraum häuften sich die Beschwerden über nicht erwünschte Telefonanrufe mit dem Ziel, Lose der Nordwestdeutschen Klassenlotterie (NKL) zu verkaufen. Die NKL mit Sitz in Hamburg ist eine staatliche Lotterie der

Länder Berlin, Brandenburg, Freie Hansestadt Bremen, Freie und Hansestadt Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Saarland, Sachsen-Anhalt und Schleswig-Holstein. Die NKL in Hamburg führt kein zentrales Kundenverzeichnis. Die Lose der NKL werden ausschließlich über ca. 90 staatlich zugelassene Lotterie-Einnahme-Stellen, sog. Lotterie-Einnahmen, in den genannten Ländern vertrieben. Diese Lotterie-Einnahmen vermarkten als selbständige Handelsvertreter die Spielangebote der NKL, nehmen den gesamten Kundenservice vor, übersenden die Lose und zahlen die Gewinne aus. Sie sind auch für die Art und Weise ihrer Werbung verantwortlich.

Einige Lotterie-Einnahmen beauftragen für Werbeaktionen externe Call-Center. Die Mitarbeiter der Call-Center werben in Telefonanrufen für den Los-Verkauf der NKL. Wie sich aus zahlreichen Beschwerden ergibt, melden sich die Anrufenden sehr oft mit dem Namen „NKL“, offenbaren dabei aber oftmals nicht, für welche NKL-Einnahmestelle die Aktion durchgeführt wird. Bei den Angerufenen entsteht so der Eindruck, die NKL mit Sitz in Hamburg sei für die Werbeaktion verantwortlich. Bei einer Nachfrage der Angerufenen, mit wem das Gespräch geführt werde und für wen der Anrufende tätig sei, wird häufig aufgelegt oder es werden auf Anfrage als Quelle für die Herkunft der Daten so genannte Zentralregister für Werbemedien angegeben, die jedoch nicht existieren.

Eine datenschutzrechtliche Überprüfung der einzelnen Beschwerden ist bei dieser verschleiernden Vorgehensweise kaum möglich, da die Beschwerdeführer in der Regel nicht mitteilen können, welche Lotterie-Einnahme für den Anruf verantwortlich ist. Die NKL selbst, auf die oftmals aggressive Werbung in ihrem Namen angesprochen, verweist darauf, dass sie keine Lose verkauft und keine Telefonkampagnen durchführt.

Die angerufenen Personen haben häufig Werbe-Klauseln angekreuzt. Diese Klauseln können Bestandteil von Bestellformularen für Zeitschriftenabonnements oder Gewinnspielformularen sein. Durch Ankreuzen des entsprechenden Kästchens wird die Erlaubnis zu telefonischer Werbung jeglicher Art erteilt. Es kommt auch oft vor, dass diese Kästchen schon mit einem Kreuz versehen sind und der Betroffene dies zur Unterbindung durchstreichen muss. Es ist zweifelhaft, ob diese Ankreuzmöglichkeit den Voraussetzungen für eine wirksame Einwilligung genügt. Oftmals liegt eine sehr große Zeitspanne zwischen dem Ankreuzen derartiger Klauseln und einem späteren Telefonmarketing, so dass für die Betroffenen ein derartiger Zusammenhang nicht mehr erkennbar ist.

Festzustellen ist: Telefonwerbung ohne Einwilligung des Betroffenen ist nach § 7 Abs. 2 Nr. 2 des Gesetzes gegen den unlauteren Wettbewerb (UWG) ein Verstoß gegen das Wettbewerbsrecht. Für die Verfolgung von Wettbewerbsverstößen sind die Verbraucherzentralen zuständig. Eine Datennutzung nach § 28

Abs. 1 Nr. 3 BDSG wäre zwar grundsätzlich zulässig, sofern die Daten allgemein zugänglich sind. Eine Nutzung der Telefonnummer z. B. aus öffentlichen Telefonverzeichnissen ist aber für Zwecke der Telefonwerbung aus datenschutzrechtlicher Sicht unzulässig, da der Betroffene aufgrund der gesetzlichen Regelung ein schutzwürdiges Interesse an dem Ausschluss der Nutzung hat.

Den Lotterie-Einnahmen ist diese Rechtslage bekannt. Auch wenn sie ein Call-Center beauftragen, in ihrem Namen für den Verkauf von Losen telefonisch zu werben, müssen sich die Lotterie-Einnahmen davon überzeugen, dass diese Werbung auf datenschutzrechtlich zulässige Art und Weise erfolgt und erforderlichenfalls von den ihnen zur Verfügung stehenden vertraglichen Sanktionsmöglichkeiten Gebrauch machen. Wer sich die Ergebnisse einer Werbeaktion zurechnen lässt, muss auch für die Art und Weise der Werbung die Verantwortung tragen. Eine Überprüfung durch die NKL, die Lotterie-Einnahmen oder die Datenschutzaufsichtsbehörden ist aber nur möglich, wenn der Name der Lotterie-Einnahme, des Call-Centers oder des Call-Center-Agenten bekannt ist. Die Nennung des Namens wird aber in vielen Fällen verweigert. Mit dieser Art und Weise der Werbung werden die Datenschutz-Rechte der Betroffenen eingeschränkt. Die Tatsache, dass NKL eine interne Telefon-Robinson-Liste führt, reicht nicht aus, um diese Rechte zu gewährleisten.

Nähere Informationen über das Telefonmarketing bei NKL können unter http://www.nkl.de/web/tele/index.html abgerufen werden.

24.2 Werbung – gar nicht witzig

Offensichtlich gibt es Werbefirmen, die vor keiner Geschmacklosigkeit zurückschrecken, um Aufmerksamkeit zu erregen. Dass sie damit auch die Privatsphäre der Betroffenen verletzen, musste ihnen erst deutlich vor Augen geführt werden.

Im Sommer 2004 ging bei der Datenschutzaufsichtsbehörde die Beschwerde einer Frau ein, die unter der Adresse ihres Arbeitgebers persönlich angeschrieben worden war. Die Sendung vermittelte den Eindruck, von einer Botschaft abgeschickt worden zu sein. Aus dem Inhalt ging hervor, dass es sich um „Green Card"-Unterlagen einer namensgleichen Person handelte, die anders nicht ermittelt werden konnte. Die persönlichen Angaben umfassten nicht nur biografische Daten sondern auch Fotos. Die Beschwerdeführerin, die sich lediglich eine Namensverwechselung vorstellen konnte, wandte sich sowohl an die Polizei als auch an den Hamburgischen Datenschutzbeauftragten. Recherchen nach dem Absender führten zunächst zu keinem Ergebnis, da nicht erkennbar war, dass es sich bei dem Absender um eine im Internet auftretende Hamburger Werbefirma handelte.

Zwei Tage später erhielt die Beschwerdeführerin ein Schreiben, aus dem hervorging, dass dies eine nach Auffassung des Unternehmens sehr wirksame Werbemaßnahme hatte sein sollen. Die Frage an das Unternehmen, woher die Daten der Beschwerdeführerin stammten, wurde dahingehend beantwortet, dass diese aus dem Internet, also einer öffentlichen Quelle, entnommen worden seien. Eine Überprüfung ergab jedoch, dass der Name der Beschwerdeführerin im Internet nicht verzeichnet war.

Das Unternehmen wurde eindringlich darauf hingewiesen, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Auch für Werbezwecke ist die Erhebung solcher Daten nur zulässig, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Nutzung hat. Dabei sind die Zwecke der Nutzung in die Betrachtung einzubeziehen. Bei derart üblen Scherzen zur Erringung der Aufmerksamkeit handelt es sich um eine unzulässige Datennutzung, selbst wenn die Daten – was im vorliegenden Fall noch nicht einmal gegeben war – dem Internet entnommen werden konnten.

25. Videoüberwachung

25.1 Videoüberwachung in Bahnen und Bussen

Die Hamburger Hochbahn AG (HHA) beabsichtigt, auch Busse mit Videotechnik auszustatten. Ein flächendeckender Einsatz von Videoüberwachung in Bussen ist datenschutzrechtlich noch nicht ausreichend begründet.

In Hamburg sind alle U-Bahnen der HHA mit Kamera- und digitaler Videoaufzeichnungstechnik ausgerüstet. Die Einzelheiten des Verfahrens sind im 19. TB, 23.2 dargestellt. Das Überwachungsverfahren ist mit dem Hamburgischen Datenschutzbeauftragten abgesprochen worden. Es erfolgt eine halbjährliche Berichterstattung an den Hamburgischen Datenschutzbeauftragten über Anlass und Umfang der zur Auswertung entnommenen Aufzeichnungen. Die HHA gibt jährlich einen Erfahrungsbericht über die Entwicklungen der Videoaufzeichnungen an den Hamburgischen Datenschutzbeauftragten. Die Videoüberwachung in den U-Bahnen ist unter Berücksichtigung der technischen Maßnahmen zur Verschlüsselung der Aufnahmen, der konkreten Dienstanweisungen an die Mitarbeiter und der weiteren datenschutzrechtlichen Vorgaben nach § 6b BDSG zulässig.

Die HHA hat testweise auch Busse mit Videotechnik ausgestattet. Wie in den U-Bahn-Wagen werden die Videoaufnahmen in den Bussen verschlüsselt auf einem digitalen Ringspeicher aufgezeichnet und automatisch nach 24 Stunden überschrieben, sofern die Festplatte nicht wegen eines zu überprüfenden

Vorfalls entnommen wird. Die HHA plant die schrittweise Ausrüstung ihrer Busse mit Videotechnik. Aus den auf unsere Anfrage hin von der HHA übersandten Unterlagen war zunächst der Wunsch der HHA zu entnehmen, diese Investitionsentscheidung zu begründen und umzusetzen. Noch nicht ausreichend begründet wurde dagegen die Erforderlichkeit dieser Maßnahme. Die Unterlagen sprachen jedoch für eine Videoüberwachung in Bussen im Abend- und Nachtverkehr.

Wir haben die HHA aufgefordert zu begründen, ob eine flächendeckende Ausstattung aller Fahrzeuge mit Video-Aufzeichnungstechnik erforderlich und aus datenschutzrechtlicher Sicht zulässig ist und dazu auf das VDV-Richtlinienpapier „ Einsatz von Videotechnik im öffentlichen Personennahverkehr (ÖPNV)“ verwiesen. Nach den dortigen Grundsätzen für den Einsatz der Videotechnik im ÖPNV darf Videoüberwachung nur zum Schutz von Personen und Beförderungseinrichtungen sowie zur technischen Fahrgastsicherheit erfolgen. Die Videoüberwachung darf nicht der Regelfall sein, sondern nur stattfinden, wenn sie notwendig ist. Es muss daher auch geprüft werden, ob den Fahrgästen die Möglichkeit einer unbeobachteten Nutzung der Verkehrsmittel eingeräumt werden kann. Es darf keine automatische Ausstattung aller Verkehrsmittel mit Videokameras erfolgen. Bei der Entscheidungsfindung über den Einsatz von Videotechnik sind die vorgesehenen Einsatzgebiete, die gewünschte Bildqualität und die innerbetriebliche Organisation zu berücksichtigen.

Das Unternehmen hat daraufhin ein Konzept zur Ausrüstung der Busse mit einem Videoaufzeichnungssystem vorgelegt. Als Gründe für die Erforderlichkeit der Videoaufzeichnungen in Bussen werden negative Entwicklungen bei der Fahrgast- und Mitarbeitersicherheit sowie die Verhinderung von Sachbeschädigungen angegeben. Es gebe eine stetige Zunahme von tätlichen Angriffen auf Busfahrer sowie von Konflikten mit Busfahrern, eine Zunahme von Konflikten zwischen Fahrgästen und von Straftaten gegenüber Fahrgästen, insbesondere in den Abend- und Nachtstunden, ferner eine Zunahme von Vandalismusschäden und die Notwendigkeit der verbesserten Nachvollziehbarkeit betrieblicher sicherheitsrelevanter Vorfälle. Die Videoüberwachung sei als präventive Maßnahme wie auch als Maßnahme zur Nachvollziehbarkeit eines Tatherganges und zur Identifikation von Tätern gerechtfertigt.

Die HHA wird zunächst bis zu 450 Busse mit Video-Aufzeichnung ausrüsten, um sicherzustellen, dass insbesondere in den Abend- und Nachtstunden ab ca. 21:00 Uhr ausschließlich Fahrzeuge mit Video-Aufzeichnung eingesetzt werden können. Nach einem Jahr ist die weitere Ausrüstung des Fuhrparks auf der Basis der gesammelten Erfahrungen mit dem Hamburgischen Datenschutzbeauftragten abzustimmen. Die Verfahrensweise für die anlassbezogene Auswertung von Aufzeichnungen orientiert sich streng an dem mit dem Hamburgischen Datenschutzbeauftragten abgestimmten Verfahren für die

U-Bahn. Analog zur U-Bahn legt die Hochbahn eine halbjährliche Berichterstattung über Anlass und Umfang der zur Auswertung entnommenen Aufzeichnungen vor. Wir halten dieses Vorgehen für vertretbar.

Im Gegensatz zu den U-Bahnen erfolgt in den S-Bahnen, die durch die S-Bahn GmbH betrieben werden, noch keine Videoüberwachung. Videotechnik wird bei der S-Bahn zur Zugabfertigung eingesetzt. Dabei werden Videoaufnahmen der an den Bahnsteigen stehenden Züge an die zentrale Zugabfertigung in Altona übertragen. Außerdem werden sicherheitsrelevante Einrichtungen wie Fahrkartenautomaten, Rolltreppen und Fahrstühle sowie Notrufsäulen dauerhaft videoüberwacht. Die Aufnahmen werden in Echtzeit von der Zugaufsicht genutzt. Eine Aufzeichnung der Aufnahmen findet nicht statt. Nach mehreren Zwischenfällen auf S-Bahn-Anlagen ist die Forderung nach einer flächendeckenden Videoüberwachung bei der S-Bahn erhoben worden. Die S-Bahn GmbH strebt zunächst eine Videoüberwachung und -aufzeichnung an 10 Stationen an. Die weitere Vorgehensweise wird mit dem Hamburgischen Datenschutzbeauftragten abgesprochen werden.

Auf Bundesebene wird derzeit unter Vorsitz des Bundesbeauftragten für den Datenschutz über eine einheitliche Handhabung des Einsatzes der Videoüberwachung im ÖPNV diskutiert. Ziel ist es, die zunehmende Videoüberwachung im ÖPNV auf das erforderliche Maß zu begrenzen und die Verkehrsbetriebe anzuhalten, auch andere, das Persönlichkeitsrecht weniger einschränkende Maßnahmen zu ergreifen, um den ÖPNV sicherer zu machen.

25.2 Videoüberwachung in Umkleidekabinen

Die leicht zu installierende Videotechnik erleichtert es den Unternehmen, ihre Kunden in allen erdenklichen Situationen zu beobachten. Selbst vor Umkleidekabinen macht der Einsatz von Kameras nicht halt.

Zunehmend erhält der Hamburgische Datenschutzbeauftragte Beschwerden von Bürgern über den Einsatz von Videoüberwachungsanlagen, die auch in Umkleidekabinen installiert werden. Mehrere Fälle betrafen Fitnesscenter, einer sogar ein Bekleidungsgeschäft. Keines der Unternehmen hatte sich im Vorwege überhaupt über die datenschutzrechtlichen Voraussetzungen und Konsequenzen informiert. Schon im 19. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten wurden unter Punkt 23. die gesetzlichen Vorgaben ausführlich dargestellt und einige Einzelfälle geschildert. Dass die Überwachung jetzt auch in derart persönliche Bereiche vordringt, lässt eine Abnahme der Sensibilität selbst für den Schutz der Intimsphäre befürchten.

Der Einsatz von Videotechnik in Umkleidekabinen von Bekleidungsgeschäften kann keinesfalls mit der Verhinderung von Diebstählen gerechtfertigt werden. Die schutzwürdigen Interessen der betroffenen Kunden, die die Möglichkeit

haben müssen, sich unbeobachtet entkleiden zu können, sind als überwiegend zu bewerten.

Die Geschäftsführer der jeweils betroffenen Fitnesscenter konnten nachweisen, dass Diebstähle aus den verschlossenen Schränken vorgekommen waren und die Überwachung der Schränke sowohl vorbeugend Diebstähle verhindert, als auch der Aufklärung der Taten dient. Die Berechtigung des Interesses an der Beobachtung der Schränke ist daher nicht von der Hand zu weisen. Gleichwohl ist auch hier das schutzwürdige Interesse der Nutzer an einem Bereich, der es ermöglicht, sich unbeobachtet umzuziehen, höher zu bewerten. In Gesprächen mit dem Geschäftsführer konnten die unterschiedlichen Interessen mit kleinen Abstrichen hinsichtlich der Bequemlichkeit für die Kunden in Einklang gebracht werden. Neben deutlichen Hinweisen auf die Videoüberwachung werden die Kameras so ausgerichtet, dass nicht der gesamte Umkleidebereich, sondern nur der Teil, der die Schränke erfasst, betroffen ist. Um den Besuchern das Ausweichen vor den Kameras zu erleichtern, wurden beobachtungsfreie Bereiche ausgeschildert. Auf diese Weise konnten die Interessen der Unternehmen an einer Diebstahlsverhinderung datenschutzgerecht berücksichtigt werden.

26. Biometrische Daten

Der Einsatz biometrischer Verfahren nimmt auch im nicht-öffentlichen Bereich deutlich zu. Immer mehr Unternehmen setzen Biometrie ein, in erster Linie zur Zugangskontrolle ihrer Geschäftsräume.

Zur Frage des Einsatzes eines biometrischen Gesichtserkennungsverfahrens bei dem Automatenspiel Mundsburg der Spielbank Hamburg (siehe hierzu eingehend 19. TB, 25.2) wurden weitere Gespräche über die datenschutzgerechte Ausgestaltung des Verfahrens mit den Vertretern der Spielbank geführt. Die Thematik wurde auch im Kreise der Obersten Datenschutzaufsichtsbehörden der Länder im Düsseldorfer Kreis erörtert. Als Ergebnis wurde festgehalten, dass die datenschutzrechtliche Zulässigkeit zumindest erfordert, dass ein ausreichend sicheres System zum Einsatz kommt, das weitgehend Fehlermeldungen ausschließt, damit es nicht zu peinlichen Situationen für völlig unbeteiligte Kunden kommen kann. Die Daten nicht betroffener Besucher sind unmittelbar nach dem Abgleich zu löschen. Darüber hinaus wird nur dann von der Zulässigkeit des Einsatzes des Systems ausgegangen, wenn die Speicherung der Referenzdaten der Spielsüchtigen mit deren schriftlicher Einwilligung erfolgt. Die Einzelheiten der Einwilligungserklärung wurden mit der Spielbank erörtert. Bisher ist das Verfahren noch nicht eingesetzt worden. Der Hamburgische Datenschutzbeauftragte wird vor einem Einsatz informiert.

Ein weiterer Anwendungsfall biometrischer Daten erfolgte in einem Sonnenstudio, das die Berechtigung zur Nutzung des Studios mittels eines Daumen-

abdrucks überprüft. Die Prüfung ergab, dass der hier verwendete Fingerabdruck nicht mit einem Fingerabdruck bei erkennungsdienstlicher Behandlung vergleichbar ist und daher für derartige Zwecke auch nicht verwendet werden könnte. Der Daumenabdruck wird nur mit Einverständnis des Kunden verwendet. Spricht sich jemand gegen das Verfahren aus, werden Alternativen zur Identifikation angeboten. Unter den dargelegten Voraussetzungen war das Verfahren nicht zu beanstanden.

Videotheken arbeiten bei der Ausleihe von Videofilmen an Automaten mit biometrischen Verfahren durch Abgleich mit Fingerabdrücken, da die Verleiher sicherstellen müssen, dass nur Berechtigte Filme ausleihen und nicht etwa Jugendliche an Videos gelangen, die erst ab 18 zugelassen sind. Sofern jemand die Automatenausleihe in Anspruch nehmen will, wird ihm ein Referenzfingerabdruck abgenommen, der nicht als Bild, sondern lediglich mit der Position charakteristischer Punkte der Fingerlinien, so genannter Templates gespeichert wird. Bei der Filmausleihe führt der Kunde seine Chipkarte in den Automaten ein und identifiziert sich durch zusätzliches Fingerauflegen. Da dem Jugendschutz hohe Bedeutung zukommt und die Kunden eingewilligt haben, ist datenschutzrechtlich bei diesem Verfahren neben sicherer Speicherung und Löschung der biometrischen Daten bei Kündigung lediglich eine grundlegende Aufklärung über das angewandte biometrische Verfahren zu Beginn der Kundenbeziehung zu fordern.

27. Gesundheit

Prüfung eines privaten Großlabors

Das private Labor speichert täglich tausende patientenbezogener Daten. Die Prüfung offenbarte Mängel bei der Umsetzung des Löschungsgebots, der Zugriffsbeschränkung und der Passwortgestaltung.

Die Prüfung eines der größten Hamburger Privatlabors machte deutlich, dass es sehr große personenbezogene Datenbestände gibt, die trotz ihrer Sensibilität bei den Betroffenen meist völlig unbekannt sind. An die 400.000 Untersuchungen führt das Labor im Jahr durch – in der Regel automatisiert. Dabei entstehen von sehr vielen Hamburgerinnen und Hamburgern gesundheitsbezogene Datenspuren (Personalien, Diagnosen, Befunde). Soweit es sich um gesetzlich versicherte Patienten handelt, rechnet das Labor direkt mit der Kassenärztlichen Vereinigung ab. Der Patient erfährt nicht, dass der behandelnde Arzt gerade dieses Labor mit der Analyse der entnommenen Blut- oder Gewebeprobe beauftragte. Nur Privatpatienten erhalten eine Rechnung des Labors.

Die Aufträge und Überweisungsscheine werden gescannt und ebenso digital gespeichert wie die Befunde. Zur Zeit der Prüfung war eine Löschung der seit 1988 aufbewahrten Daten nicht vorgesehen. Dies verstößt gegen das Bundes-

datenschutzgesetz. Es fordert, dass die Daten, deren Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist, zunächst – d.h. während der zehnjährigen Aufbewahrungspflicht nach der ärztlichen Berufsordnung – gesperrt und anschließend gelöscht werden. Dieser Mangel wiegt umso schwerer, als alle Mitarbeiterinnen und Mitarbeiter des Labors einen unbeschränkten Lese-Zugriff auf die Daten haben – auch soweit sie Jahrzehnte zurück reichen. Zudem entsprach der Passwortschutz nicht den üblichen Standards.

Weiter mussten wir beanstanden, dass es für das Reinigungspersonal in der langen Zeit ohne Aufsicht durch Labormitarbeiter durchaus möglich ist, die in offenen Kästen verwahrten Überweisungsscheine nach „missbrauchsgeeigneten“ Patienten zu durchsuchen.

Schließlich ergab unsere Prüfung, dass 10 Arbeitsplätze des lokalen EDV-Netzes mit dem Internet verbunden waren, ohne dass das Laborinformationssystem ausreichend gegen Angriffe aus dem Internet gesichert war.

Die ermittelten Mängel bilden zwar keine akute Bedrohung für die gespeicherten Patientendaten. Die latente Gefährdung muss jedoch zügig beseitigt werden, weil eventuelle Missbräuche schwer erkannt werden können und die betroffenen Patienten selbst in der Regel noch nicht einmal von der Existenz der sie betreffenden Daten wissen.

Wir sind derzeit im Dialog mit der Leitung des Großlabors, um die notwendigen Maßnahmen abzustimmen.

28. Vereine

Veröffentlichung von Daten der Vereinsmitglieder im Internet

Das Internet bietet für Vereine große Chancen zur Selbstdarstellung, birgt aber auch Risiken für die Vereinsmitglieder. Vereine sollten bei der Nutzung des Mediums Internet sehr sorgfältig prüfen, welche personenbezogenen Informationen ihrer Mitglieder im Internet wirklich notwendig sind.

Das Internet wird von Vereinen und Verbänden zunehmend nicht nur zur Selbstdarstellung genutzt, sondern auch zur Veröffentlichung von Spielergebnissen, Mannschaftsaufstellungen und Ranglisten. Nicht alle Vereinsmitglieder finden diese Veröffentlichungen gut. Der Adressatenkreis im Internet ist unbegrenzt und einmal in das Internet eingestellte Daten sind dauerhaft preisgegeben, da die Daten weltweit abrufbar sind. Bei der Nutzung des Internets muss daher abgewogen werden, ob und welche personenbezogenen Daten zur Veröffentlichung im Internet notwendig sind.

Mehrere Beschwerden richteten sich gegen die Veröffentlichung von Spielerdaten auf der Website des Hamburgischen Fußballverbandes (HFV). Satzungsgemäß veröffentlicht der HFV bei Erteilung einer Spielberechtigung in

einem zum HFV gehörenden Verein im Internet folgende Spielerdaten: Name, Vorname, Verein, Spielerpass-Nr., Datum der Erteilung einer Spielberechtigung für Pflicht- / Freundschafts- / Pokalspiele. Bei der Verhängung einer Spielsperre bzw. einer anderen Strafe durch die Rechtsorgane des HFV werden Name, Vorname, Verein, Spielerpass-Nr., Datum des Spiels, Zeitraum der Sperre, Strafmaß, Zeitpunkt der Aussetzung zur Bewährung, Verhängung aufgrund Feldverweis ja / nein veröffentlicht.

Rechtsgrundlage für die Veröffentlichung dieser personenbezogenen Daten der Spieler ist deren Einwilligung, die beim Eintritt in den Verein eingeholt wird. Im Antragsformular des HFV befindet sich vor der Unterschrift ein deutlicher Hinweis auf die auf der Rückseite des Antrags abgedruckten „Hinweise zum Datenschutz", die die Vorgehensweise bei der Veröffentlichung von Daten detailliert erklären.

Die Einwilligung des Spielers kann grundsätzlich jederzeit widerrufen werden. Die Nichterteilung der Einwilligung oder deren Widerruf bewirkte in der Vergangenheit jedoch nach den Bestimmungen der Satzung gleichzeitig den Verlust der Ausübung bestimmter mit der Datenerhebung verbundener Rechte innerhalb des HFV, z. B. Wahrnehmung der Spielberechtigung bzw. Ausübung des Schiedsrichter- oder Traineramtes. Diese Vorgehensweise hatte der HFV mit dem Hamburgischen Datenschutzbeauftragten vor einigen Jahren abgesprochen. Hiergegen wandten sich die Beschwerdeführer, die geltend machten, dass sie gezwungen seien, der Veröffentlichung ihrer personenbezogenen Daten im Internet zuzustimmen, wenn sie in Hamburg Fußball spielen wollten.

Aufgrund der Beschwerden wurde im Düsseldorfer Kreis mit den übrigen Datenschutzaufsichtsbehörden erörtert, ob und unter welchen Voraussetzungen andere Verbände oder Vereine, die dem DFB angehören, Spielerdaten im Internet veröffentlichen. Es stellte sich heraus, dass aufgrund eines ähnlichen Falles im Jahr 2001 das Regierungspräsidium Darmstadt mit dem DFB vereinbart hatte, dass aus datenschutzrechtlichen Gründen die Weigerung eines Spielers, einer Veröffentlichung seiner Daten im Internet zuzustimmen, zu keinen Nachteilen für den Spieler führen dürfe. Hintergrund war, dass die Einwilligung nach § 4 a Abs. 1 BDSG auf der freien Entscheidung des Betroffenen beruhen muss und nicht durch den ansonsten drohenden Entzug der Spielerlaubnis erzwungen werden darf. Der DFB hatte seine Mitgliedsverbände in einem Rundschreiben entsprechend informiert.

Das Ergebnis der Erörterung im Düsseldorfer Kreis wurde dem HFV mitgeteilt, der daraufhin seine Satzung änderte. Danach bedarf es weiterhin einer jederzeit widerrufbaren Einwilligung des Mitglieds für die Veröffentlichung seiner Daten im Internet. Der Widerruf der Einwilligung hat für die Mitglieder jedoch keine nachteiligen Konsequenzen mehr.

Eine weitere Beschwerde betraf die Veröffentlichung von Spielergebnissen im Internet und die Erstellung von Ranglisten durch einen Tennisverein, ohne dass vorher die Einwilligung der Spieler und Spielerinnen eingeholt wurde. Der Beschwerdeführer rügte, dass aus den veröffentlichten Daten das gesamte Urlaubs- und Freizeitverhalten der Spieler ersichtlich sei. Nach überwiegender Auffassung der im Düsseldorfer Kreis vertretenen Datenschutzaufsichtsbehörden ist die Veröffentlichung von Spielergebnissen, Mannschaftsaufstellungen und Ranglisten mit den Namen der aktiven Spielerinnen und Spieler im Internet auch ohne deren Einwilligung nach § 28 Abs.1 Nr. 3 BDSG zulässig. Die von einem Verein ausgerichteten Veranstaltungen sind öffentlich. Die Namen und die Ergebnisse der Aktiven werden im Rahmen dieser Veranstaltung öffentlich bekannt gegeben, so dass es sich um allgemein zugängliche Daten handelt. Die Daten der Ranglisten stellen eine Zusammenfassung und Auswertung dieser öffentlich zugänglichen Daten dar.

Anhaltspunkte dafür, dass das schutzwürdige Interesse der Spielerinnen und Spieler an einem Ausschluss der Veröffentlichung gegenüber dem berechtigten Interesse des Vereins offensichtlich überwiegt, sind nicht ersichtlich. Zwar lassen sich die Daten im Internet für einen unbegrenzten Teilnehmerkreis erschließen und stehen anders als bei anderen Medien zumeist über einen längeren Zeitraum zur Verfügung. Auch ist nicht ausgeschlossen, dass die Daten für andere Zwecke genutzt werden (z. B. Werbezwecke). Dennoch gehen die Datenschutzaufsichtsbehörden nicht davon aus, dass eine Internetveröffentlichung der genannten Daten die Persönlichkeit der Spielerinnen und Spieler mehr beeinträchtigt als deren Veröffentlichung in einer Tageszeitung, in deren Verbreitungsgebiet sie wohnen. Allerdings dürfen bei den Veröffentlichungen im Internet nur Nachname, Vorname, Vereinszugehörigkeit und eventuell, falls erforderlich, der Geburtsjahrgang aufgeführt werden. Die Veröffentlichung des Geburtsdatums oder der privaten Anschrift wäre dagegen nach § 28 Abs. 1 Nr. 3 BDSG unzulässig, da die schutzwürdigen Interessen der Betroffenen entgegenstünden. Die Veröffentlichung dieser Daten wäre nur mit ausdrücklicher Einwilligung der Spielerinnen und Spieler zulässig.

29. Bußgeldfälle und Strafanträge

Im Berichtszeitraum wurden in fünf Fällen Bußgelder festgesetzt und zwei Strafanträge gestellt.

Vier Bußgeldverfahren betrafen dieselbe verantwortliche Stelle, da trotz mehrfacher Aufforderung zur Auskunftserteilung gegenüber der Aufsichtsbehörde für den Datenschutz nicht reagiert bzw. die Auskunft nicht vollständig erteilt wurde (§ 43 Abs. 1 Nr. 10 BDSG). Gegen eine andere verantwortliche Stelle musste ebenfalls wegen Auskunftsverweigerung ein Bußgeld festgesetzt werden. Die Höhe der Bußgelder lag in 3 Fällen bei € 350,00, zweimal wurde € 1.500,00 verhängt.

Die Aufsichtsbehörde für den Datenschutz hat in zwei Fällen erstmalig von ihrem Recht, Strafantrag zu stellen, Gebrauch gemacht. In einem Fall wurden unbefugt Patientenadressen übermittelt. Der zweite Strafantrag richtet sich gegen die Inhaber einer Auskunftei, die unbefugt personenbezogene Daten über das Zahlungsverhalten von Kunden erhebt und verarbeitet (§ 43 Abs. 2 Nr. 1 BDSG).

30. Meldepflicht und Prüftätigkeit

30.1 Meldepflicht und Register nach § 4d BDSG

Die Zahl der Meldungen ist wiederum gestiegen.

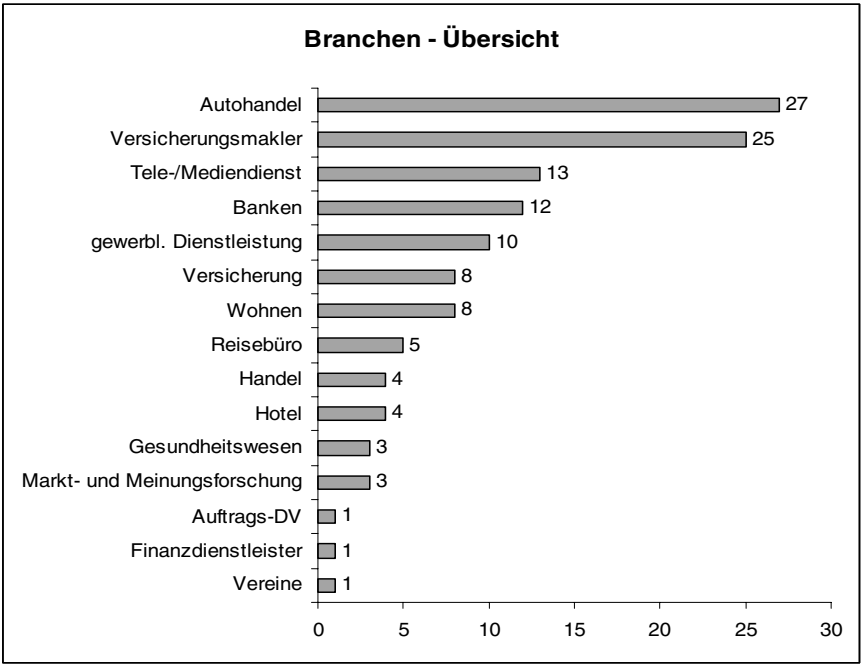
Die Aufsichtsbehörde führt nach § 38 Abs. 2 BDSG ein Register der Stellen, die nach § 4d BDSG der Meldepflicht unterliegen. Bisher haben 38 Unternehmen ihre Angaben zur Meldepflicht entsprechend den Vorgaben des § 4e BDSG angepasst oder sich zum ersten Mal zum Register gemeldet (vgl. 18. TB, 29.1, 19. TB, 27.1). Unterteilt nach der Art der meldepflichtigen Verfahren ergibt sich folgendes Bild:

- Speicherung zum Zwecke der Übermittlung:
  - Auskunfteien / Warndienste 10
  - Informationsdienste 4
  - Adresshändler 3
- Speicherung zum Zwecke der anonymisierten Übermittlung:
  - Markt- und Meinungsforschung 21

30.2 Prüfungen

Die Prüfungen von nicht öffentlichen Stellen sind fortgesetzt worden.

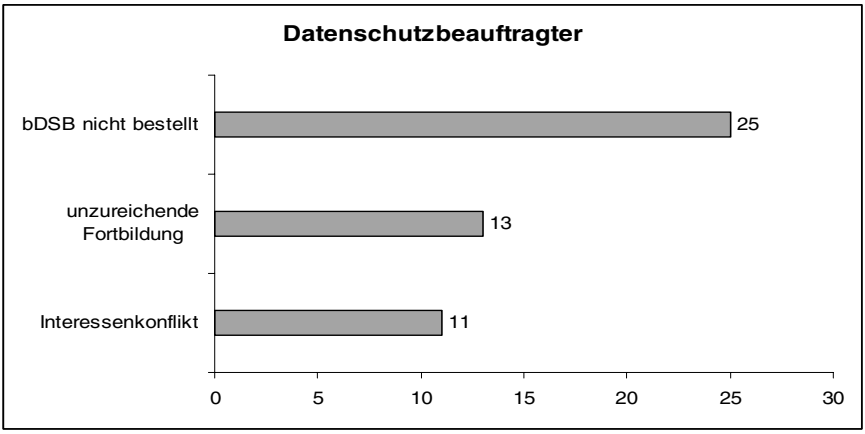
Die im aktuellen Bundesdatenschutzgesetz vom Mai 2001 neu aufgenommene Regelung der anlassfreien datenschutzrechtlichen Kontrolle von nicht öffentlichen Stellen ermöglichte uns seit 2002 eine umfangreichere Datenschutzaufsicht als zuvor. Aufgrund reduzierter Personalressourcen mussten wir den Prüfungsumfang allerdings verringern. Schwerpunkt der Prüfungen im Berichtszeitraum von November 2003 bis einschließlich Dezember 2005 bildete auch weiterhin die Kundendatenverarbeitung. Gegenüber den Vorjahren haben wir die Anzahl geprüfter Branchen deutlich erweitert. Insgesamt wurden 125 Unternehmen geprüft.

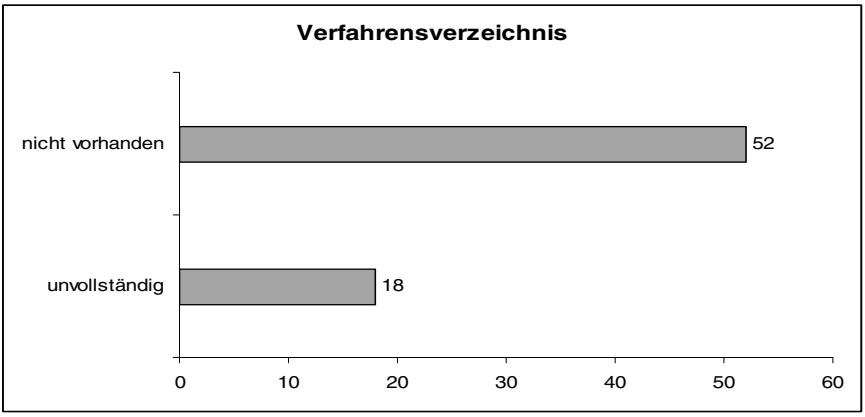


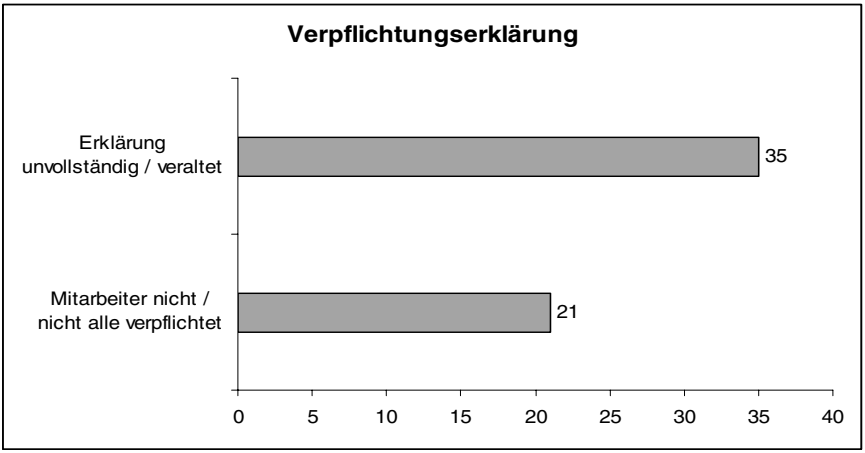
Gegenstand der Prüfungen war, außer bei Tele- und Mediendiensten:

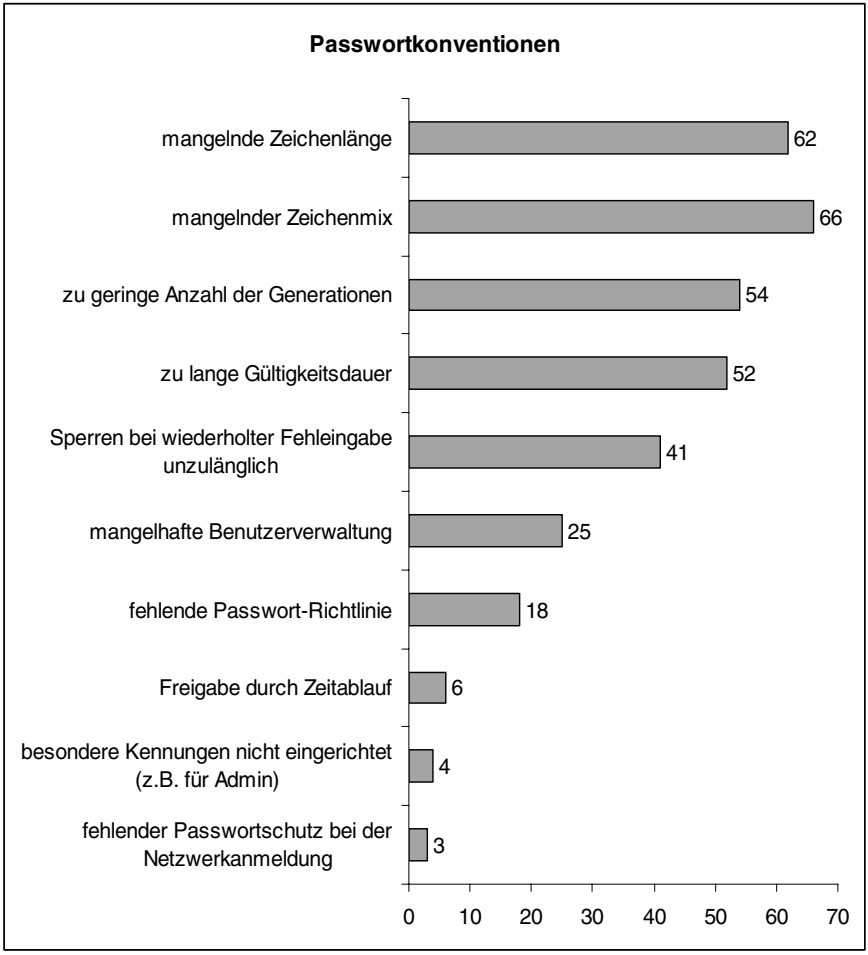
- die Verpflichtung zur Bestellung eines Datenschutzbeauftragten nach § 4f BDSG und seine Fachkunde nach § 4g Abs. 1 BDSG,
- das Verfahrensverzeichnis nach § 4g Abs. 2 BDSG,
- die Verpflichtung auf das Datengeheimnis nach § 5 BDSG,
- die technischen und organisatorischen Maßnahmen nach § 9 BDSG,
- die Auftragsdatenverarbeitung nach § 11 BDSG,
- die Meldepflicht nach § 4d BDSG.

Keine der durchgeführten Prüfungen konnte ohne einen Mängelbericht abgeschlossen werden. Im Folgenden sind die überprüften Themenbereiche mit ihren wesentlichsten Mängeln dargestellt.

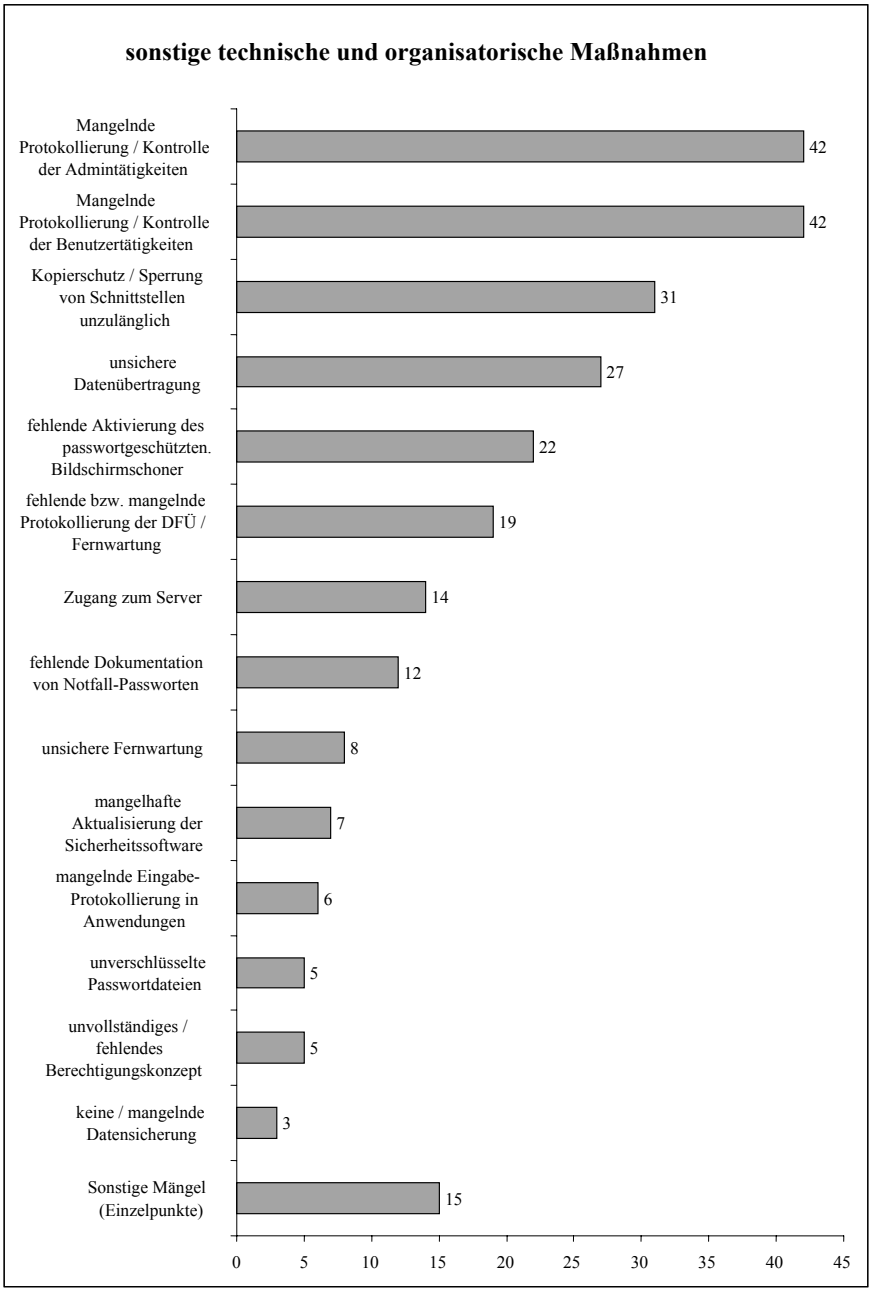

Datenschutzbeauftragter
bDSB nicht bestellt
25
unzureichende Fortbildung
13
Interessenkonflikt
11
0
5
10
15
20
25
30

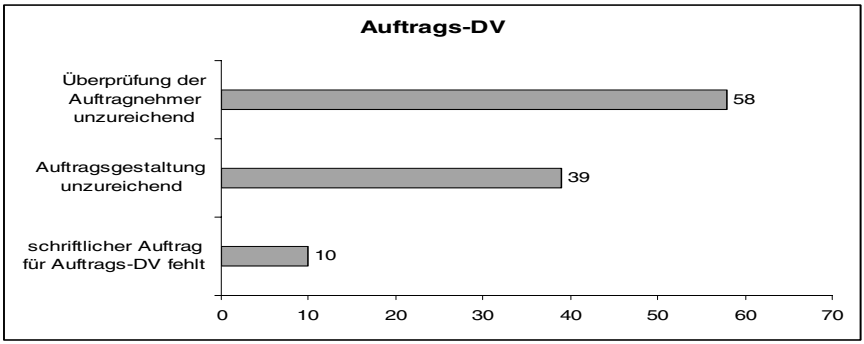

Verfahrensverzeichnis
nicht vorhanden
52
unvollständig
18
0
10
20
30
40
50
60


Verpflichtungserklärung
Erklärung unvollständig / veraltet
35
Mitarbeiter nicht / nicht alle verpflichtet
21
0
5
10
15
20
25
30
35
40



Zahlreiche Anwendungen bei den geprüften Unternehmen waren nur unzureichend gegen unberechtigte Zugriffe gesichert. Die Empfehlungen zum IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik – BSI – wurden nur unzureichend berücksichtigt.


sonstige technische und organisatorische Maßnahmen
Mangelnde Protokollierung / Kontrolle der Admintätigkeiten
42
Mangelnde Protokollierung / Kontrolle der Benutzertätigkeiten
42
Kopierschutz / Sperrung von Schnittstellen unzulänglich
31
unsichere Datenübertragung
27
fehlende Aktivierung des passwortgeschützten. Bildschirmschoner
22
fehlende bzw. mangelnde Protokollierung der DFÜ / Fernwartung
19
Zugang zum Server
14
fehlende Dokumentation von Notfall-Passworten
12
unsichere Fernwartung
8
mangelhafte Aktualisierung der Sicherheitssoftware
7
mangelnde Eingabe-Protokollierung in Anwendungen
6
unverschlüsselte Passwortdateien
5
unvollständiges / fehlendes Berechtigungskonzept
5
keine / mangelnde Datensicherung
3
Sonstige Mängel (Einzelpunkte)
15
0
5
10
15
20
25
30
35
40
45



Die Anzahl festgestellter Mängel bestärkt uns in dem Vorhaben, auch weiterhin per Zufallsprinzip ermittelte Firmen im Hinblick auf den technisch-organisatorischen Datenschutz zu prüfen. Bei über 50 % der geprüften Unternehmen mussten wir ein nicht vorhandenes oder unzulängliches Verfahrensverzeichnis bemängeln. Ähnliches gilt für die Kontrolle der so genannten Auftragsdatenverarbeiter.

Immerhin 20 % der kontrollierten Firmen hatten, trotz gesetzlicher Verpflichtung, keinen betrieblichen Datenschutzbeauftragten bestellt. Obwohl das aktuelle Datenschutzrecht in erster Linie eine Selbstkontrolle der Wirtschaft vorsieht, verdeutlichen die vorliegenden Zahlen die Notwendigkeit einer begleitenden Kontrolle durch die Aufsichtsbehörde.

BÜRGERSERVICE UND DIENSTSTELLE

31. Eingaben

Die hohe und steigende Zahl der Eingaben, die an die Dienststelle herangetragen werden, belegt, dass Datenschutz von den Bürgerinnen und Bürgern sehr wichtig genommen wird, aber leider sowohl bei den öffentlichen als auch bei den nicht öffentlichen Stellen noch nicht den notwendigen Stellenwert erreicht hat oder auch – teilweise aus Unkenntnis – nicht beachtet wird. Unsere Einschaltung führt in der Regel zu dem notwendigen Interessenausgleich im Einzelfall.

Anhand der jahresweise erfassten Zahl der Eingaben zeigte sich der weiterhin hohe Stand der Fälle, in denen sich Bürgerinnen und Bürger schriftlich an uns wenden. Von Dezember 2004 bis Dezember 2005 gingen 1.216 Eingaben ein.

Sie betrafen – getrennt für die Jahre 2004 und 2005 – folgende Datenschutzbereiche:

	2004	2005
Versicherungswirtschaft	37	26
Kreditwirtschaft	12	24
Priv. Wohnungswirtschaft	14	18
Versandhandel	11	8
sonst. Handel	20	32
Werbung, Direktmarketing	86	116
Schufa, Auskunfteien	35	40
Markt- und Meinungsforschung	1	10
Vereine	8	11
Freie Berufe	46	15
Soziales u. Gesundheitsw., nicht-öff.	14	18
Personaldatenschutz, nicht-öff.	13	18
Verkehrswesen, nicht-öff.	6	3
Sonstiges, nicht-öff.	14	42
Justiz	16	14
Strafvollzug	15	9
Verfassungsschutz	4	15
Polizei	24	36
Staatsanwaltschaft	9	4
Meldewesen	13	12
Wahlen	6	3
MDK, Kranken- und Pflegedienste	5	7
andere Sozialbereiche	43	42
Gesundheitswesen, öff.	12	9
Personaldatenschutz, öff.	11	14
Verkehrswesen, öff.	9	12
Ausländerwesen	5	4
Finanz- und Steuerwesen	4	12
Bildungswesen	9	17
Wirtschaftsverwaltung	1	-
Telekommunikation	19	15
Tele- und Mediendienste	44	36
Medien	3	7
Personenstandswesen	1	3
Statistik	1	4
Bau- und Vermessungswesen	4	4
Hochschulen	2	4
Scientology	1	-
Sonstiges, öff.	8	16
Umweltschutz	3	2
Abgaben	58	33
Insgesamt Eingaben:	**569**	**647**

32. Beratungen und Informationsangebote

Die Zahl der Beratungen und der Prüfungen durch die Dienststelle ist weiterhin hoch. Unsere Informationsangebote wurden von den Bürgerinnen und Bürgern intensiv genutzt.

Im Berichtszeitraum haben wir insgesamt 2.850 Bürgerinnen und Bürger, die sich persönlich, telefonisch oder schriftlich mit ihren Fragen und Problemen zum Datenschutz an uns gewandt haben, beraten (2004 ca. 1.500 Fälle, 2005 ca. 1.350 Fälle).

Die Beratungen für öffentliche und nicht öffentliche Stellen beliefen sich im Jahr 2004 auf über 1.500 Fälle und im Jahr 2005 auf rund 1.400 Fälle. Außerdem prüften wir im Jahr 2004 in über 320 Fällen und im Jahr 2005 in knapp 350 Fällen öffentliche und nicht öffentliche Stellen. In rund 110 Fällen im Jahr 2004 und in rund 180 Fällen im Jahr 2005 gaben wir Stellungnahmen zu Datenschutzfragen in Rechts- oder Verwaltungsvorschriften ab.

Wie in den Vorjahren wurden unsere Informationsmaterialien in großem Umfang nachgefragt. Die Handreichungen und Materialien wurden zunehmend über unser Internet-Angebot abgerufen (www.datenschutz.hamburg.de).

Dienststelle (Stand: 1. Februar 2006)

Der Hamburgische Datenschutzbeauftragte
Klosterwall 6, 20095 Hamburg
E-Mail: mailbox@datenschutz.hamburg.de
Internet-Adresse: www.datenschutz.hamburg.de

Tel: 040 / 42854-4040
Fax: 040 / 42854-4000

		Durchwahl
Dienststellenleiter:	Hartmut Lubomierski	– 4041 –
Stellvertreter:	Dr. Hans-Joachim Menzel	– 4049 –
Vorzimmer:	Heidi Niemann	– 4040 –
Geschäfts- und Verwaltungsangelegenheiten der Dienststelle	Rolf Nentwig	– 4043 –
Informationsmaterial	Irene Heinsohn	– 4042 –
	Heidi Niemann	– 4040 –
IuK-Leitung und IuK-Planung, Internetangebot der Dienststelle	Martin Schemm	– 4044 –
Grundsatzfragen des Datenschutzrechts, Datenschutzgesetze, Parlamentsangelegenheiten, Justiz, Strafvollzug, Verfassungsschutz, Sicherheitsüberprüfungen, Ausweis- und Passangelegenheiten, Archivwesen	Dr. Harald Wollweber	– 4045 –
Statistik, Personenstandswesen, Meldewesen, Finanz-, Steuer- und Rechnungswesen	Gunnar Hansen	– 4046 –
Polizei, Feuerwehr, Staatsanwaltschaft	Herbert Janßen	– 4047 –
Gesundheitswesen, Forschung, Kultur, Telekommunikations-, Rundfunk- und Presserecht, Bauen und Wohnen, Umwelt, Arbeitskreis Medien	Dr. Hans-Joachim Menzel	– 4049 –

Stichwortverzeichnis