Tätigkeitsbericht 2008/2009

Der Hamburgische Beauftragte
für Datenschutz und Informationsfreiheit

Hamburg

22. Tätigkeitsbericht des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zugleich Tätigkeitsbericht der Aufsichtsbehörde für den nicht-öffentlichen Bereich 2008 / 2009

vorgelegt im Februar 2010

Prof. Dr. Johannes Caspar
(Redaktionsschluss: 31. Dezember 2009)

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

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

Auflage: 1.200 Exemplare

Druck: Lütcke & Wulff, 22525 Hamburg

INHALTSVERZEICHNIS

Vorwort

Die im Zeitraum des Tätigkeitsberichts 2008-2009 beschriebenen Aktivitäten fallen zur Hälfte in die Amtszeit meines Vorgängers, [redacted] der bis zum Jahresende 2008 als Hamburgischer Datenschutzbeauftragter die Dienststelle leitete. Für den Zeitraum vom 1.1.2009 bis zu meinem Amtsantritt am 4.5.2009 wurde die Leitungsfunktion dann übergangsweise von meinem Stellvertreter, [redacted] wahrgenommen. Dank ihrer im Berichtszeitraum geleisteten hervorragenden Arbeit, die angesichts diverser Datenschutzmängel und -skandale durch große Herausforderungen geprägt war, wurde mir die Übernahme des neuen Amtes als Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit sehr erleichtert.

Meinen Mitarbeiterinnen und Mitarbeitern danke ich für ihren sachkundigen und engagierten Einsatz zur Stärkung und Fortentwicklung des Datenschutzes und für den Aufbau des Anfang 2009 hinzugekommenen Sektors der Informationsfreiheit.

In den kommenden Jahren stehen wir vor entscheidenden Weichenstellungen sowohl in den unterschiedlichen Schwerpunkten des Datenschutzes als auch auf dem innovativen Feld der Informationsfreiheit. Im 2. Halbjahr 2009 haben wir erforderliche Umstrukturierungen eingeleitet und das Konzept Hamburger Datenschutz 2010 erarbeitet, das neue Impulse zur Gestaltung einer die Persönlichkeitsrechte wahrenden Informations- und Kommunikationsordnung setzt.

Gemeinsam sollte es uns gelingen, den Datenschutz auch in schweren Zeiten auf einem guten und erfolgreichen Kurs zu halten. Ebenso sollte es uns gelingen, die Bürgerinnen und Bürger bei der Wahrnehmung ihrer Informationsfreiheit zu unterstützen und die hamburgischen Behörden für jedermann transparent zu machen.

Prof. Dr. Johannes Caspar

Februar 2010

I. Konzept Hamburger Datenschutz 2010

1. Einleitung

In dem Maße, wie die Digitalisierung der Gesellschaft voranschreitet, gewinnt auch der Datenschutz an Bedeutung. Die Entwicklung moderner Überwachungstechnologien, aber auch die neuen Entwicklungen des Internet sowie die Möglichkeiten immer einfacherer Kopierbarkeit und schnellerer Übertragung von Daten stellen enorme Anforderungen an den grundrechtskonformen Schutz des informationellen Selbstbestimmungsrechts sowie an die technische Ausgestaltung der Datensicherheit.

Um diesen Herausforderungen gerecht zu werden, müssen Datenschutzbehörden zu multifunktionalen Wirkeinheiten werden, die zunächst ihre Kontrollverantwortung und Überwachungsfunktionen im öffentlichen Interesse ausüben und gleichzeitig als Dienstleistungs- und Servicebetrieb für die Durchsetzung der Grundrechte von Bürgerinnen und Bürgern tätig werden. Daneben gehört es zu ihrem Selbstverständnis wie auch zu ihrem gesetzlichen Anforderungsprofil, über den gesamten Querschnittsbereich behördlicher und privater Datennutzung beratend und aufklärend tätig zu werden. Sie haben dafür zu sorgen, dass sowohl bei den Betroffenen als auch bei den verantwortlichen Stellen das Bewusstsein für den Datenschutz und damit eine grundsätzliche Bereitschaft zur Einhaltung datenschutzrechtlicher Anforderungen besteht.

Die vielfältigen Ansätze, aber auch die hohe rechtliche sowie technische Komplexität des Datenschutzes und der Datensicherheit verlangen eine Spezialisierung der Dienststelle sowohl im nicht-öffentlichen, als auch im öffentlichen Bereich. Gleichzeitig sind aber unsere personellen sowie finanziellen Ressourcen begrenzt. Zur Sicherung der künftigen Handlungs- und Gestaltungsfähigkeit der Dienststelle auf einem der technischen Entwicklung der Informationsgesellschaft entsprechenden Niveau erscheint es künftig erforderlich, ein nachhaltiges Konzept zu entwickeln, mit dem wir auch in Zukunft für eine persönlichkeitsgerechte Informationsordnung eintreten können.

2. Bestandsaufnahme – Die gegenwärtige Situation des Hamburger Datenschutzes

Die Erstellung eines intelligenten und zukunftsfähigen Konzepts „Hamburger Datenschutz 2010" hat zunächst bei einer kritischen Bestandsaufnahme anzusetzen. Prägend für die derzeitige Situation der Dienststelle sind zwei miteinander verwobene Entwicklungen: die zunehmende Befassung mit datenschutzrechtlichen Defiziten bei nicht-öffentlichen Stellen (2.1) und eine erhebliche Steigerung der von Bürgerinnen und Bürgern bei der Dienststelle eingelegten Eingaben (2.2).

2.1 Auf dem Weg zur privaten Überwachungsgesellschaft?

Vor dem Hintergrund einer stetig voranschreitenden Digitalisierung der Gesellschaft ergibt sich bei einem absoluten Anstieg der datenschutzrechtlich relevanten Fälle eine deutliche Tendenz zur Verlagerung der Datenschutzanforderungen vom öffentlichen auf den nicht-öffentlichen Bereich, das heißt vom staatlichen Sektor auf die privatwirtschaftlichen Akteure. Diese Entwicklung ist keine landesspezifische Besonderheit. Vielmehr vollzieht sie sich sowohl im internationalen als auch im nationalen Rahmen im Windschatten des Fortschritts der Informations- und

Kommunikationstechnologie sowie einer zunehmenden kommerziellen Nutzung personenbezogener Daten. Dies belegen die zahlreichen im Berichtszeitraum dokumentierten Datenschutzskandale in und außerhalb Hamburgs, über die ausführlich in den Medien berichtet wurde.

Treffend brachte Prof. Dr. Papier, der Präsident des Bundesverfassungsgerichts, diese Entwicklung aus Anlass der Festveranstaltung des 25. Jahrestages des Volkszählungsurteils zum Ausdruck, indem er feststellte: „Mittlerweile haben sich die technischen Möglichkeiten der Datenverarbeitung freilich so sehr revolutioniert, dass der ‚große Bruder" George Orwell's aus heutiger Sicht über die damals, gewissermaßen in der informationstechnischen Steinzeit bestehenden Möglichkeiten der Überwachung nur noch mitleidig lächeln könnte. Die technischen Möglichkeiten von heute befinden sich allerdings nicht mehr in den Händen weniger Einzelner oder gar nur von Staaten. Die Privatisierung der Informationstechnologie hat im Zusammenhang mit der Globalisierung die Zahl potentieller ‚Big Brother' so unübersichtlich werden lassen, dass aus datenschutzrechtlicher Sicht anarchische Zustände eher zu drohen scheinen als ein totalitärer Überwachungsstaat."[1]

Auch wenn die Regelungen zur Online-Durchsuchung, zum Kfz-Screening oder zur Vorratsdatenspeicherung den Datenhunger der Sicherheitsbehörden von Bund und Ländern längst noch nicht gestillt haben, auch wenn die informationelle Selbstbestimmung und das jüngst durch die Entscheidung zur Online-Durchsuchung des Bundesverfassungsgerichts neu konzipierte Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme bis an die Grenze der Rechtsstaatlichkeit und teilweise darüber hinaus durch Gesetzgeber und Exekutive ausgereizt werden: Es ist zu konstatieren, dass gerade private Stellen im Berichtszeitraum in steigendem Maße die tägliche Arbeit der Datenschutz- und Aufsichtsbehörden bestimmt haben.

Die überproportionale Befassung mit Datenschutz im nicht-öffentlichen Bereich der Dienststelle wird durch unsere Eingabenstatistik belegt. Als Eingaben gelten alle schriftlichen Beschwerden oder Bitten von Bürgerinnen und Bürgern, die uns auf dem Postweg, über Fax oder E-Mail zugehen, die zur Verfolgung von Individualinteressen erhoben werden und eine schriftliche Bearbeitung erfordern. Danach ist in den letzten Jahren der Anteil der schriftlichen Beschwerden gegen Daten verarbeitende private Stellen, die bei uns eingingen, kontinuierlich gestiegen. Richteten sich die Beschwerden bis zu Beginn der 1990er Jahre lediglich in 43% der Fälle an nicht-öffentliche Stellen, so hat sich das Verhältnis bis 2009 mittlerweile umgekehrt. Nunmehr haben 80% aller Eingaben das Verhalten oder Unterlassen eines privaten Akteurs zum Gegenstand, so dass eine Zuständigkeit der Aufsichtbehörde nach § 38 BDSG besteht (siehe TB IV 12).

2.2 Eingabenbearbeitung – Aufgabe mit immer höherem Aufwand

In zunehmender Weise wird die Arbeit der Dienststelle durch Eingaben von Bürgerinnen und Bürgern nicht nur aus der Stadt Hamburg, sondern auch aus anderen Bereichen in Deutschland geprägt. Mitunter werden wir auch mit Anliegen aus dem Ausland befasst. Zum Bereich des Datenschutzes ist seit Anfang 2009 auch der Bereich der Informationsfreiheit hinzugekommen, dessen Eingaben statistisch getrennt aufgeführt werden.

[1] Papier, Das Volkszählungsurteil des Bundesverfassungsgerichts, in: 25 Jahre Volkszählungsurteil. Datenschutz – Durchstarten in die Zukunft, hrsg. vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, S. 13, 15.

Die Eingaben im Bereich des Datenschutzes im letzten Zehnjahreszeitraum haben sich verdoppelt: Im Jahr 2000 hatte die Dienststelle noch 509 Eingaben zu verzeichnen. Von 2001 bis 2007 lagen die Eingaben konstant zwischen 542 (im Jahr 2003) und 690 (im Jahr 2007). Ab diesem Zeitraum ist eine signifikante Steigerung zu verzeichnen: Im Jahre 2008 gab es bereits 848 Eingaben. 2009 ist nun zum ersten Mal eine vierstellige Zahl zu verzeichnen: Der Dienststelle lagen Ende 2009 1115 Eingaben vor (s. Eingabenjahresstatistik TB IV. 12). Der Anstieg ist nicht mit der seit dem 28. Februar 2009 bestehenden neuen Funktion der Behörde für den Bereich der Informationsfreiheit erklärbar. Hier hat es im Berichtszeitraum bis Ende Dezember lediglich 19 Eingaben gegeben. Das Referat Informationsfreiheit arbeitet konzeptionell an einer stärkeren Verankerung der Möglichkeiten und Rechte der Informationsfreiheit im Bewusstsein von Bürgerinnen und Bürgern und bemüht sich damit perspektivisch um eine stärkere Auslastung gerade durch Eingaben auf diesem Sektor.

Die Entwicklung im Bereich der Eingaben auf dem Gebiet des Datenschutzes ist durchaus ambivalent: Zum einen ist die Aufgabe, zur Wahrnehmung der Rechte von Bürgerinnen und Bürgern gegenüber öffentlichen und privaten Stellen tätig zu werden, mit dem Selbstverständnis des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit unmittelbar verbunden: Die Befassung mit schriftlichen Beschwerden und Bitten durch Bürgerinnen und Bürger war in der Vergangenheit ein zentraler Arbeitsschwerpunkt unserer Dienststelle. Diese Bedeutung wird die Eingabenbearbeitung auch in Zukunft haben.

Zum anderen bindet die Zunahme der Eingaben jedoch auch in immer stärkerem Maße die Arbeitskraft der Dienststelle. Hier droht die Gefahr einer Überlastung und Blockade bei den übrigen Aufgaben unserer Dienststelle. Dies gilt gerade vor dem Hintergrund, dass die sprunghafte Entwicklung der Eingabenzahlen einem personellen Rückgang in den letzten Jahren für den Bereich des Datenschutzes gegenübersteht: Verfügte die Dienststelle Ende 2001 noch über 16,63 Stellenanteile, so liegt die derzeitige Zahl bei 14,70. Zwei jüngst hinzugekommene neue Stellen wurden für den Bereich der Informationsfreiheit eingerichtet und lassen sich nicht dem Bereich „Datenschutz" hinzurechnen.[2]

Im Rückblick auf den Berichtszeitraum war eine deutliche Tendenz der isolierten Befassung der Mitarbeiterinnen und Mitarbeiter mit Einzelfällen zu spüren, die zu einer deutlich Fixierung der Dienststelle auf bereits festgestellte Verstöße führte. Die starke Ausrichtung der einzelnen Referentinnen und Referenten auf die Bearbeitung von Eingaben bindet große Anteile der Kapazitäten, die für übergreifende Maßnahmen in Richtung auf einen präventiv angelegten Datenschutz dringend benötigt würden. Zwar können sich Eingaben mitunter als geeignete Indikatoren zur Aufdeckung von generell dysfunktionalen Strukturen erweisen. Dennoch bleibt unsere Dienststelle bei der Bearbeitung von individuellen Rechtsverfolgungsbegehren weitgehend auf reaktives Verhalten beschränkt; es fehlt ein übergreifendes Konzept für ein frühzeitiges Eingreifen der Datenschutzbehörde und eine Präventionsstrategie, die die verschiedenen Referate untereinander, aber auch die einzelnen Referatsmitarbeiter stärker verbindet. Die hohe Auslastung der Dienststelle mit der Eingabenbearbeitung erschwert die Entwicklung von übergreifenden Konzepten behördlicher Kontrolle und Steuerung. Infolgedessen muss der Rückgang an-

[2] Unzutreffend daher die jüngst durch die Studie der Xamit Bewertungsgesellschaft, Datenschutzbarometer 2009 – kein Datenschutz in Deutschland, S. 28, ausgewiesenen Stellenanteile für den Bereich des HmbBfDI, die auch die Stellen für die Informationsfreiheit mit einbezieht.

lassunabhängiger Prüfungen in den letzten Jahren durchaus auch als Reaktion auf die Zunahme der Einzelanliegen der Bürgerinnen und Bürger angesehen werden.

Die personelle Ausstattung der Dienststelle entspricht nicht der gewachsenen Bedeutung des Datenschutzes in Wirtschaft, Gesellschaft und Staat. Die Mehrlast an Eingaben war im Berichtszeitraum nur durch den motivierten Einsatz aller Mitarbeiter der Dienststelle zu bewältigen. Ein weiteres Ansteigen, aber auch ein Verbleib auf dem derzeitigen Niveau von über 1000 Eingaben p.a. dürfte sich auf Dauer nicht ohne Vernachlässigung anderer Aufgabenschwerpunkte bewältigen lassen. So ist im Berichtszeitraum ein Rückgang der anlassunabhängigen Kontrollen durch die Dienststelle zu verzeichnen, der jedoch im 2. Halbjahr 2009 gestoppt werden konnte (dazu die statistischen Angaben zur Prüftätigkeit TB IV. 11). Wir werden die weitere Entwicklung genau analysieren und daran anknüpfend gegebenenfalls konkrete Forderungen für eine Verbesserung der Stellenausstattung unterbreiten.

2.3 Zunahme von IT-Projektbegleitungen im öffentlichen Bereich – Herausforderung an den technischen Datenschutz

Parallel zu der Zunahme von Eingaben ist auch der Einsatz von IT in der öffentlichen Verwaltung im Berichtszeitraum stark angestiegen. Neben einigen Großvorhaben, die unter anderem eine erhebliche Umstrukturierung von Verwaltungsabläufen mit dem Ziel einer papierlosen Verwaltung mit sich bringen, gibt es eine Vielzahl kleinerer Projekte, die gleichfalls Fragen nach Datenschutz und Datensicherheit aufwerfen.

Zu den größeren Projekten zählen HIM und Eldorado, die der Schaffung eines einheitlichen elektronischen Dokumentenmanagementsystems in der hamburgischen Verwaltung dienen und erhebliche Auswirkungen auf den Zugriff der Daten innerhalb der Hamburger Verwaltung haben. Ebenso sind hier zu nennen die Projekte ePers und koPers, die auf eine komplette Neuausrichtung der IT-Unterstützung von Personalmanagementaufgaben ausgerichtet sind, ferner das neue Verfahren der Mittelbewirtschaftung und Anlagenbuchhaltung der Freien und Hansestadt Hamburg sowie das Projekt einer elektronischen Patientenakte (Soarian). Auf weitere IT-gestützte Anwendungsverfahren, deren Federführung bei unterschiedlichen Behörden liegt, wird in den einzelnen Abschnitten des Tätigkeitsberichts verwiesen.

Anlässlich der Einführung von neuer IT in den verschiedenen Bereichen der hamburgischen Verwaltung bemühen wir uns um einen präventiven Beratungsansatz, der auf eine möglichst frühzeitige Beteiligung unseres technischen Sachverstands setzt. Nur durch eine bereits im Projektplanungsstadium wirksame Beteiligung können nachträgliche und unter Umständen aufwändige Korrekturen vermieden werden. Im Grundsatz erkennt auch die Hamburger Verwaltung die Vorteile einer begleitenden Beratung durch den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit an und kommt unserem Anliegen einer frühzeitigen Beteiligung entgegen. In der Praxis bedeutet dies aber auch, dass über längere Planungszeiträume hinweg unsere Beratungspräsenz im Rahmen von Abstimmungs- und Planungsprozessen gefordert ist. Die Folge ist eine zeitintensive Einbindung in komplexe Verfahren, bei denen wir jedoch die Möglichkeit für Verbesserungen des Datenschutzes und der Datensicherheit gern wahrnehmen. Dies erscheint allerdings nur unter einer reduzierten Prüftätigkeit bereits eingeführter Verfahren möglich.

2.4 Bedarf für ein strategisches Zukunftskonzept

Die Zunahme der Eingaben, aber auch der Wunsch der Behörden nach einer möglichst frühen Beteiligung an neuen IT-Projekten stellen positive Indikatoren für die öffentliche Akzeptanz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit dar. Offensichtlich wird der Datenschutz als ein wichtiges Anliegen wahrgenommen. Die stärkere öffentliche Beachtung von Fragen zum rechtlichen und technischen Datenschutz sowie der Datensicherheit macht jedoch auch eine Problemdimension sichtbar: Mit Sorge erfüllt uns, dass die Zunahme von Beschwerden der Bürgerinnen und Bürger auch ein beträchtliches tatsächliches Defizit an Datenschutz in Gesellschaft und Staat belegt. Die deutliche Zunahme der an uns herangetragenen Beschwerden zeigt, dass der Stellenwert des Datenschutzes bei vielen öffentlichen und auch bei privaten Stellen noch verbesserungsbedürftig ist.

Angesichts knapper personeller Ressourcen und angesichts eines erheblichen Bedeutungszuwachses von Datenschutz und Datensicherheit gegenüber öffentlichen und nichtöffentlichen Stellen müssen neue Wege beschritten und Strategien entwickelt werden, um einer Blockade der Dienststelle durch ein weiteres Ansteigen der Eingabenbearbeitung entgegenzuwirken. Dies erfordert in weiten Teilen eine kritische Überprüfung der derzeitigen Organisationsstrukturen und der Verfahrensabläufe, aber auch ein neues Selbstverständnis bei der Kontrolle der Einhaltung des Datenschutzrechts. Hier setzt das Konzept Hamburger Datenschutz 2010 an.

3. Strategische Ausrichtung des Konzepts Hamburger Datenschutz 2010

Unter den geschilderten Bedingungen muss ein richtungsweisendes Konzept des Datenschutzes die vorhandenen Ressourcen auf die Stärkung von Datenschutzkompetenz und Eigenverantwortung sowohl bei den Daten verarbeitenden Stellen, als auch bei den von der Datenverarbeitung betroffenen Bürgerinnen und Bürgern bündeln. Mit simplen Top-to-Bottom Regelungs- und Vollzugsstrategien können die vielfältigen, sich im Querschnittsbereich gänzlich diverser gesellschaftlicher wie auch staatlicher Akteure und Funktionsbereiche ergebenden Fragestellungen des Datenschutzes nicht (mehr) adäquat gelöst werden.

Das Konzept Hamburger Datenschutz 2010 sieht für die künftige Aufgabenerfüllung daher drei im Grundsatz gleichberechtigte Module vor, die sich gegenseitig ergänzen und deren Ziel es ist, die Stärkung und den Vollzug der Regelungen des Datenschutzrechts auf unterschiedliche Weise durch die Behörde zu verfolgen: Zwei der Konzepte beruhen auf der Aktivierung und Stimulierung der Kompetenzen zur Selbststeuerung und richten sich in erster Linie an das aufgeklärte Eigeninteresse der Akteure. Das dritte Modul setzt auf die hierarchische Steuerungsebene des Rechts und damit auf die Zwangs- und Drohkompetenz einer staatlichen Aufsicht, ohne die ein Rechtsvollzug nicht gewährleistet werden kann.

3.1 Modul 1 – Stärkung der Kompetenzen zum Selbstdatenschutz

Die Fähigkeit der Bürgerinnen und Bürger zum Selbstdatenschutz ist Voraussetzung für das eigenverantwortliche und aufgeklärte Verhalten in der digitalen Informationsgesellschaft. Zum Modul Selbstdatenschutz im Rahmen des Konzepts Hamburger Datenschutz 2010 zählen alle Maßnahmen staatlicher Aufgabenträger, die darauf abzielen, die Kompetenzen des Einzelnen zum Schutz und zur Durchsetzung seines informationellen Selbstbestimmungsrechts sowie seines Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

zu stärken, und zwar unter rechtlichen, technischen und organisatorischen Aspekten. Die Fähigkeit zum aktiven Datenmanagement setzt ein an Datenschutz wie auch Datensicherheit ausgerichtetes Verhalten des Einzelnen voraus. Hierzu gehören zum einen das Wissen über die Gefährdungen der personenbezogenen Daten und zum anderen die Kenntnisse, um aktiv Maßnahmen zum Selbstschutz und zur selbständigen Rechtsverfolgung ergreifen zu können.

Maßnahmen zur Stärkung des Selbstdatenschutzes richten sich in erster Linie als Informationsangebote an die Bereitschaft des Einzelnen, sich reflexiv mit den Folgen seines Handelns unter Datenschutzaspekten zu beschäftigen. Sie beruhen daher auf Freiwilligkeit und nicht auf staatlichem Zwang.

3.1.1 Aufklärung/Information der Öffentlichkeit

Zu den vielfältigen Möglichkeiten, die in diesem Bereich ergriffen werden können, zählen Angebote zur Aufklärung über den sicheren technisch-organisatorischen Umgang mit den eigenen Daten sowie Informationen über die eigenen Datenschutzrechte und die Möglichkeiten und Wege der Betroffenen, diese gegenüber den Daten verarbeitenden öffentlichen wie auch nicht-öffentlichen Stellen geltend zu machen. Neben allgemeinen, der Orientierung dienenden Handreichungen („12 Tipps zum Datenschutz") sind häufig gerade Informationen über den Datenschutz in bestimmten Bereichen notwendig, die Hinweise geben, künftig mit den persönlichen Daten in einer selbstverantwortlichen Weise umzugehen.

Die Dienststelle wird sich künftig verstärkt durch gezielte Informationsangebote sowohl im Internet als auch durch Flyer, Medienpublikationen und Fachaufsätze an die Öffentlichkeit wenden. Dabei soll verstärkt Wert darauf gelegt werden, besonders über eingabenrelevante Bereiche genauer und breiter als in der Vergangenheit zu unterrichten. Hier kommen statistisch besonders häufig auftretende Fragestellungen, etwa zum Adresshandel, zum Surfen im Internet oder zur Zulässigkeit der Videoüberwachung im öffentlichen wie auch im nicht-öffentlichen Bereich in Betracht.

Auch wenn eine unmittelbar spürbare Entlastung durch Aufklärungskampagnen nicht erreicht werden kann – so sollte eine präventive Beratung und das Vorhalten von Aufklärungs- und Informationsmaterial doch zumindest dazu führen, dass sich sowohl bei den Daten verarbeitenden Stellen, als auch bei den davon Betroffenen eine stärkere Ausrichtung des Verhaltens auf eine rechtlich zulässige Praxis einstellt. So wäre es als Erfolg zu werten, wenn die Zahlen der Eingaben, denen eine hinreichende tatsächliche und rechtliche Basis fehlen, und der tatsächlichen Verstöße gegen den Datenschutz durch die verantwortlichen Stellen infolge der Informationen künftig zurückgingen.

3.1.2 „Meine Daten kriegt ihr nicht!" – Initiative zur Datenschutzkompetenzförderung an Schulen

Ein wichtiges Feld des Selbstdatenschutzes eröffnet sich für die Dienststelle künftig im Bereich der Datenschutzkompetenzförderung von Schülerinnen und Schülern. Datenschutz ist auch eine Bildungsaufgabe. Gerade die junge Generation sollte in die Lage versetzt werden, sich sicher und verantwortungsvoll in der virtuellen Welt zu bewegen. Wir haben bereits die Weichen für ein Projekt gestellt, das in den kommenden Jahren zu einer festen Einrichtung an Hamburger Schulen werden soll.

Problemstellung:

Die digitale Gesellschaft konfrontiert Kinder und Jugendliche mit Risiken, die sie ohne ein technisches, aber auch soziales Sinnverständnis der Zusammenhänge nicht bewältigen können. Die Erfahrungen, die sie im virtuellen Raum machen, entziehen sich häufig auch dem Erfahrungshorizont ihrer Eltern. Längst kann die Weitergabe von Wissen innerhalb der Familie als Ort kulturellen Lernens kaum mehr geleistet werden. Zu rasant ist die Entwicklung der Informationsgesellschaft.

Bislang findet im schulischen Alltag eine Vermittlung des Basiswissens über den Umgang mit den eigenen Daten im Internet nicht oder bestenfalls am Rande statt. Ohne die Risiken zu kennen, ohne überhaupt ein Bewusstsein für Gefahren der virtuellen Welt zu haben, wachsen Schülerinnen und Schüler unvorbereitet und oft auch sorglos in ihre Rolle als „digital natives": Für ihre Hausarbeiten recherchieren sie im Internet, in ihrer Freizeit besuchen sie Chat-Rooms, sind Mitglieder von sozialen Netzwerken und betreiben eigene Internetseiten. Die vielfältigen Möglichkeiten der digitalen Selbstdarstellung im Internet kennen keine Grenzen und die Kinder und Jugendlichen leider oft auch keine selbstkritische Reflektion.

Gerade in der schulischen Ausbildung müsste das informationelle Selbstbestimmungsrecht sich zu einer Schutzpflicht des Staates verdichten, die darauf gerichtet ist, die Fähigkeiten zum Selbstdatenschutz zu stärken. Hier ist staatliches aktives Tun gefordert. Staatliche Stellen sollten deshalb ihrer Verantwortung für die Grundorientierung der Schülerinnen und Schüler für einen sicheren Einstieg und Aufenthalt in der virtuellen Welt stärker als bisher nachkommen. Dies betrifft nicht nur die Schulen und die staatlichen Stellen, die sich mit der Organisation von Schule beschäftigen. Gefordert sind gerade auch die in sachlicher Hinsicht zuständigen Datenschutzbehörden mit ihrem Fachwissen.

An der Vermittlung der Grundkompetenz für ein eigenverantwortliches Datenmanagement bei Schülerinnen und Schülern mitzuwirken, ist daher ein zentrales Anliegen des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit. Wir haben deshalb das Projekt „Meine Daten kriegt ihr nicht!" initiiert, um unseren Beitrag bei der Stärkung der Datenschutzkompetenz der Schülerinnen und Schüler zu leisten und für ein vertieftes Verständnis des Datenschutzes auch bei jungen Menschen einzutreten. Für die Entwicklung der Datenschutzkompetenz sollen künftig die allgemeinbildenden Schulen einen wichtigen Beitrag leisten.

Zum Begriff „Datenschutzkompetenzförderung":

Der Begriff der Datenschutzkompetenzförderung stellt auf den ersten Blick einen Unterbegriff zur allgemeinen Medienkompetenzförderung dar, geht jedoch inhaltlich über diesen hinaus. Beide Begriffe weisen eine dreipolige Begriffsstruktur auf: Neben einer technisch-funktionalen Fähigkeit (nutzungsbezogen) und einer kognitiv-interpretatorischen Fähigkeit (verständnisbezogen) ist damit eine kognitiv-kritische Fähigkeit gemeint, die wertungs- und urteilsbezogen ist.

Für die Datenschutzkompetenzförderung sind im nutzungs- und verständnisbezogenen Kontext zunächst die Fragen „Was geschieht mit meinen Daten?" und „Wie kann ich einen Missbrauch meiner Daten verhindern?" maßgebend. Im Bereich des kognitiv-kritischen Bedeutungsgehalts stellt sich darüber hinaus die Frage: "Was soll ich schützen?"

Während die Medienkompetenzförderung in erster Linie eine technisch-instrumentelle Komponente aufweist, hat der Begriff Datenschutzkompetenzförderung einen starken reflexiven Gehalt: Es geht um den Einsatz eigener Ressourcen, der eigenen Daten. Diese geben Auskunft über die Persönlichkeit und Einzigartigkeit des Individuums. Entscheidend ist hier die Sicht auf die eigene Person, der Bezug zu sich selbst, der das Datenschutzmanagement des Einzelnen wesentlich beeinflusst.

Unsere Initiative beabsichtigt nicht, mit erhobenem Zeigefinger eine besondere Form der Selbstdarstellung gerade von Kindern und Jugendlichen zu kritisieren oder abzuwerten. Die Neigung, mit den eigenen Daten freigiebig umzugehen, mag in hohem Maße abhängig von Alter und kultureller Prägung sein. Sie setzt jedoch die individuelle Freiheit der Entscheidung voraus. Ohne die Einsichtsfähigkeit des Einzelnen in die Folgen des Verzichts auf seine Datenintegrität kann von einem freien und selbstverantwortlichen Handeln nicht gesprochen werden. Damit Kinder und Jugendliche mit ihren eigenen Daten eigenverantwortlich umgehen können, müssen sie ein Bewusstsein für die zahlreichen Risiken und Nachteile haben, die mit einem freigiebigen Datenmanagement in der modernen Informationsgesellschaft verbunden sein können. Denn nur wer die Konsequenzen seines individuellen Verhaltens überblicken kann, ist auch in der Lage, eine eigenverantwortliche Entscheidung über die Weitergabe seiner Daten zu treffen.

Projektziele:

Wir wollen unsere vielfältigen Kenntnisse und Erfahrungen in den Prozess der Erarbeitung von Lehrkonzepten, der Weitergabe im Rahmen der Lehrerausbildung sowie der Durchführung von Pilotprojekten und Aktionswochen einbringen. Ziel des Projekts „Meine Daten kriegt ihr nicht!" ist es, Schülerinnen und Schülern in der Freien und Hansestadt Hamburg die erforderlichen Kenntnisse für einen eigenverantwortlichen Umgang mit ihren persönlichen Daten in der Welt des Internet zu geben. Dabei geht es nicht nur darum zu lernen, verantwortungsvoll mit den eigenen Daten, sondern auch respektvoll mit den Daten anderer Menschen umzugehen. Der missbräuchlichen Datenverwendung gerade in dieser Altersgruppe – hier seien nur die Beispiele Cyber-Mobbing und Cyber-Grooming genannt – soll damit genauso entgegengewirkt werden wie dem Hang zu einem allzu freizügigen Umgang mit den eigenen Daten, was mit zahlreichen Gefahren sozialer sowie ökonomischer Nachteile verbunden ist.

Ziel des Pilotprojekts soll es sein, den Grundstein zu legen für die Implementierung eines modernen Konzepts zur Förderung der Datenschutzkompetenz in die Ausbildung der allgemeinbildenden Schulen Hamburgs. Im weiteren Verlauf sollen die Erfahrungen, die im Rahmen des Pilotprojekts gemacht wurden, in die Fortentwicklung des Projekts einfließen. Damit die Datenschutzkompetenzförderung allen Schülerinnen und Schülern an Hamburger Schulen zuteil wird, ist die Schulbehörde gefragt. Wir werden sie nach unseren Kräften unterstützen. Die Verstetigung des Wissenstransfers und dessen Fluss in alle Schulen hinein setzt aber maßgeblich auch das Engagement der Lehrerinnen und Lehrer an Hamburgs Schulen voraus. Ihre Bereitschaft, sich künftig mit Fragen des Datenschutzes zu beschäftigen und diese an ihren Schulen in den Unterricht einzubringen, wird letztlich darüber entscheiden, ob es in naher Zukunft gelingt, allen Hamburger Schülerinnen und Schülern das Wissen weiterzugeben, das erforderlich ist, damit diese sich als selbstverantwortliche Akteure durch die digitale Welt bewegen können.

Projektkooperationspartner:

Um einen wirksamen und effektiven Zugang zu der Zielgruppe herzustellen, ist das Projekt auf unterschiedliche Kooperationspartner angewiesen. Dies gilt zunächst für die öffentlichen Stellen der Freien und Hansestadt Hamburg, die einen Beitrag zur Ausbildung von Schülerinnen und Schülern leisten.

In diesem Zusammenhang war es entscheidend, dass wir für eine Kooperation die Schulsenatorin gewinnen konnten. Durch die Zusammenarbeit mit der Behörde für Schule und Berufsbildung sowie dem ihr zugeordneten Landesinstitut für Lehrerbildung und Schulentwicklung soll künftig die Verankerung der Datenschutzinhalte in den medienpädagogischen Unterricht, die Erarbeitung von Lehrkonzepten sowie die Einbringung der Datenschutzkompetenzförderung in die Lehrpläne möglich werden.

Unterstützt wird das Projekt ferner durch den Innensenator der Freien und Hansestadt Hamburg. Das Landeskriminalamt fungiert als zuständiger Kooperationspartner für die Kriminalprävention in internet- und jugendaffinen Bereichen (Einbettung von Erscheinungsformen der Internetkriminalität, bei denen Kinder und Jugendliche statistisch häufig Opfer werden).

Begleitend erfolgt eine Beteiligung der Medienanstalt Hamburg Schleswig-Holstein aufgrund ihrer Zuständigkeit für den Jugendmedienschutz.

Als Medienkooperationspartner konnten wir den NDR gewinnen, der zeitnah über das Projekt und seinen Fortgang berichten wird. Über die unterschiedlichen Altersgruppen, die der NDR mit seinen Programmen erreicht, kann das notwendige Bewusstsein der Öffentlichkeit für die Medienkompetenzförderung und für ein selbstverantwortliches Datenmanagement bei Schülerinnen und Schülern geschärft werden.

Das Konzept soll der Öffentlichkeit am 8. Februar 2010 zum Safer-Internet-Day im Rahmen eines Pilotprojekts an einer Hamburger Schule vorgestellt werden. Die Wahl der Schule fiel auf die Gesamtschule Walddörfer im Nordosten Hamburgs: Die Entscheidung gewährleistet eine schulartunabhängige Einbeziehung der Schülerinnen und Schüler und ermöglicht gleichsam, dass die zahlreichen Erfahrungen, die die Gesamtschule im Bereich der Medienkompetenzförderung in der Vergangenheit sammeln konnte, dem Pilotprojekt zu Gute kommen.

Ausblick:

Nach Abschluss der Pilotphase wird es darauf ankommen, das Projekt auszuwerten und die Erfahrungen und Erkenntnisse in die hamburgweite Umsetzung einfließen zu lassen. Wir sind uns bewusst, dass unsere Behörde eine Verstetigung des Wissenstransfers in die Lehrerfortbildung nicht leisten kann, die erforderlich wäre, um alle Hamburger Schulen in voller Breite zu erreichen. Wir werden aber allen Akteuren unsere Hilfe anbieten, das Thema künftig in der Lehrerfortbildung zu verankern. Insbesondere in Zusammenarbeit mit dem Landesinstitut für Lehrerbildung und Unterrichtsentwicklung werden wir unseren Teil zur Weiterverbreitung des Themas in die Hamburger Schulen beitragen.

3.2 Modul 2 – Datenschutz als Aufgabe betrieblicher und behördlicher Selbstverantwortung

In der demokratischen Informationsgesellschaft ist eine Totalkontrolle durch Datenschutzbehörden weder gewünscht, noch ist sie aufgrund der Personalausstattun-

gen der Datenschutzbehörden möglich. Von daher kommen den tragenden Prinzipen der Eigenverantwortung und der Freiwilligkeit Daten verarbeitender Stellen eine wichtige Funktion für ein intelligentes Konzept der modernen Verhaltenssteuerung zu. Aufsichtsbehördliches Einschreiten sollte nur die letzte aller möglichen Optionen sein, rechtskonformes Verhalten zu bewirken. Neben den traditionellen Instrumentarien von Überwachung, Vollzug und Sanktion bleibt daher die Aktivierung der autonomen Steuerungskompetenzen datenverarbeitender Stellen eine Option, auf die die Datenschutzbehörden künftig setzen müssen.

Sowohl nicht-öffentliche wie auch öffentliche Stellen haben ein Eigeninteresse, die Aufgabe des Datenschutzes möglichst eigenverantwortlich, möglichst ohne nachsteuernde Eingriffe von außen und ohne Sanktionsdruck zu erfüllen. Es gilt daher, bereits vorhandene Instrumente der regulierten Selbstregulierung weiter auszubauen und dort, wo dies möglich ist, Anreize für die eigenverantwortliche Übernahme von Datenschutzaufgaben zu schaffen.

3.2.1 Betriebliche Selbststeuerung im nicht-öffentlichen Bereich

Die zahlreichen Datenpannen und Datenmissbräuche der letzten Jahre, mit denen Unternehmen ganz unterschiedlicher Branchen in das Licht der Öffentlichkeit gerieten, dokumentieren ein erschreckendes Defizit an Professionalität im Umgang mit dem Datenschutz, gerade auch mit Fragen der Datensicherheit. Dass ein selbstverantwortliches, präventives Datenschutzmanagement im Dienst von Kunden und Verbrauchern den Unternehmen im Wettbewerb durchaus helfen kann, ist eine Einsicht, die leider noch längst nicht überall das betriebliche Denken und Handeln bestimmt.

Wir werden in Zukunft verstärkt bei den Unternehmen mit Hauptsitz in der Freien und Hansestadt Hamburg dafür werben, den Datenschutz und die Sicherheit von Kundendaten nicht als lästige Pflichtaufgabe zu verstehen, für die es sich betriebswirtschaftlich nicht rechnet, Ressourcen einzusetzen. Vielmehr sollen hier die Erkenntnis und das Bewusstsein vermittelt werden, dass Schutz und Sicherheit von Kundendaten für die Glaubwürdigkeit sowie die Wettbewerbsfähigkeit von Unternehmen eine wichtige Größe sind. Das belegen sowohl die in Datenschutzfragen zunehmend sensibilisierte Öffentlichkeit, als auch eine steigende Zahl von Unternehmen, die sich bei uns nach Beratungs- und Schulungsmöglichkeiten im Bereich des Datenschutzes erkundigen.

Betrieblicher Datenschutzbeauftragter:

Eine Schlüsselrolle für die Stärkung der Eigenverantwortlichkeit datenverarbeitender Stellen innerhalb der Betriebe kommt den von den Unternehmen nach Maßgabe des § 4f Bundesdatenschutzgesetz (BDSG) zu bestellenden betrieblichen Datenschutzbeauftragten zu. Die Beauftragten werden von uns künftig stärker als Partner im Bemühen um einen effizienten Datenschutz einbezogen werden. Gerade eine betriebsinterne Vorprüfung der Eingaben von Betroffenen kann durchaus in eine Win-Win-Situation zwischen Datenschutzbehörde, Bürger und Daten verarbeitendem Unternehmen münden: Über die betrieblichen Datenschutzbeauftragten erkennen die Daten verarbeitenden Stellen datenschutzrelevante Defizite und können interne Maßnahmen zur Beseitigung implementieren. Neben der Möglichkeit des betriebsinternen Clearings durch eine technische und organisatorische Schwachstellenanalyse erhalten Betriebe somit die Option, rechtliche Maßnahmen der Aufsichtsbehörde durch eigenverantwortliches Datenschutzmanagement

rechtzeitig abzuwenden und damit auch mögliche Bußgeldsanktionen zu vermeiden.

Das Einschalten betrieblicher Datenschutzbeauftragter kann gleichzeitig eine schnelle und unbürokratische Abhilfe der Beschwerden von Betroffenen bewirken und damit deren Rechte wahren, ohne dass behördliche Ressourcen in Anspruch genommen werden müssen. Die Verlagerung der Eingabenbearbeitung in ein betriebsinternes „Vorverfahren" verschafft daher allen Beteiligten Vorteile und hilft, langwierige Verfahren zu vermeiden.

Gesetz zum Datenschutz-Audit:

Damit Datenschutz und Datensicherheit tatsächlich im Wettbewerb zwischen den Unternehmen wirksam werden können, müssen sich die Kunden bei der Entscheidung über einen Vertragsschluss mit einem externen IT-Dienstleister an verlässlichen Maßstäben über den tatsächlich gewährleisteten Datenschutz solcher Unternehmen ausrichten können. Für Zertifizierungen von Produkten oder Unternehmen sind klare gesetzliche Vergabekriterien erforderlich, die durch unabhängige Gutachter überprüft werden. Neben der intensiven Nutzung und Stärkung der betrieblichen Datenschutzbeauftragten werden wir künftig dafür eintreten, dass das für die Aufwertung des Datenschutzes im Wettbewerb zentrale Instrument des Datenschutz-Audits künftig durch den (Bundes-)Gesetzgeber eine verbindliche und transparente Regelung erfährt.

Gerade der Fall eines Hamburger Internet-Buchhändlers, bei dem trotz eines kurz zuvor auch für Datenschutz und Datensicherheit erteilten TÜV-Prüfsiegels mehrere hunderttausend Kundendaten problemlos im Internet abgerufen werden konnten, dokumentiert, dass transparente Kriterien für die Zertifizierung von Unternehmen bislang fehlen (dazu s. unter IV 7.3). Ohne gesetzliche Standards bei der Zertifizierung bleibt der Datenschutz aus Verbrauchersicht ein Muster ohne Wert und kann in weiten Bereichen eine Vertragsentscheidung für den Kunden nicht rational begründen oder ausschließen. Es bedarf daher transparenter und klarer gesetzlicher Vorgaben, damit künftig zertifizierte Unternehmen oder Produkte tatsächlich das Vertrauen ihrer Kunden verdienen.

3.2.2 Behördliche Datenschutzbeauftragte – intelligentes, aber noch zu wenig genutztes Instrument behördlicher Eigenkontrolle

Anders als im nicht-öffentlichen Bereich fehlt für öffentliche Stellen im Hamburgischen Datenschutzgesetz eine verbindliche Bestellungspflicht für behördliche Datenschutzbeauftragte. Die von uns im letzten Tätigkeitsbericht angeregte gesetzliche Regelung hierzu wurde leider nicht aufgegriffen (vgl. 21. TB, S. 36f). Es ist daher nach wie vor den öffentlichen Stellen überlassen, ob und für welche Bereiche ein Datenschutzbeauftragter bestellt werden soll. Die Bestellung auf Basis einer freiwilligen Entscheidung der Behördenleitung hat zu einer uneinheitlichen Praxis in der hamburgischen Verwaltung beim Einsatz von behördlichen Datenschutzbeauftragten geführt (zum Sachstand siehe Tätigkeitsbericht unter III. 1).

Vorteile für alle Beteiligten:

Unsere Empfehlung geht dahin, künftig den Datenschutz im öffentlichen Bereich durch die Bestellung von Datenschutzbeauftragten zu stärken. Die Erfahrungen in der Zusammenarbeit mit behördlichen Datenschutzbeauftragten sind aus unserer Sicht für alle Akteure durchweg positiv verlaufen. Dort, wo behördliche Datenschutzbeauftragte bestellt wurden, haben sich diese für den Hamburgischen Be-

auftragten für Datenschutz und Informationsfreiheit als kompetente und verlässliche Partner erwiesen. Für die öffentlichen Stellen erweist sich die Bestellung von Datenschutzbeauftragten vor allem als Hilfe bei der Bewältigung der oft umfangreichen und komplexen Datenschutzaufgaben, die gerade auch zu einer Entlastung anderer mit dem Datenschutz zusätzlich befasster Referenten in der Linie der behördlichen Funktionseinheiten führen kann.

Mit dem verstärkten Einsatz von weisungsfreien Datenschutzbeauftragten in Hamburger Behörden (zum Überblick aller Behörden, die einen Datenschutzbeauftragten bestellt haben, s. unter III. 1) ergibt sich auch für den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit die Hoffnung, künftig die Eingaben von Bürgerinnen und Bürgern zumindest in einigen Fällen in einem vorgeschalteten Verfahren an die behördlichen Datenschutzbeauftragten als behördeninterne Clearingstelle abzugeben. Hierin liegt eine Chance für die Verwaltung, Defizite beim Datenschutz durch autonome Abhilfeentscheidungen bereits intern zu korrigieren.

Gleichzeitig führte eine Bestellung von behördlichen Datenschutzbeauftragten regelmäßig zu einer Verringerung der externen Kontrolle durch die Datenschutzbehörde: So ist die sogenannte Risikoanalyse nach § 8 des Hamburgischen Datenschutzgesetzes (HmbDSG) dem behördlichen Datenschutzbeauftragten zuzuleiten. Die Verfahrensbeschreibung nach § 9 HmbDSG ist von ihm zu führen und zur Einsicht bereit zu halten. Ist kein Beauftragter bestellt, sind die Verfahrensbeschreibungen und Risikoanalysen von der verantwortlichen Stelle dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit vorzulegen.

Es wird angestrebt, künftig in stärkerem Maße die Erfüllung dieser technisch-organisatorischen Verpflichtungen zu kontrollieren und auch deren ordnungsgemäße Durchführung zu prüfen. Für die öffentlichen Stellen sollte dies ein zusätzlicher Anreiz sein, künftig eigene Datenschutzbeauftragte zu bestellen, die diese Aufgaben mit Fachkunde und Zuverlässigkeit behördenintern bewältigen.

Förderungsprogramm für behördliche Datenschutzbeauftragte:

Uns ist bewusst, dass im Regelfall die Bestellung von Behördenmitarbeitern als behördliche Datenschutzbeauftragte einer längeren, von den individuellen Kenntnissen abhängigen Einarbeitungs- und Eingewöhnungsphase bedarf. Wenngleich § 10a Abs. 2 HmbDSG bestimmt, dass nur Personen mit der notwendigen Fachkunde als behördliche Datenschutzbeauftragte bestellt werden dürfen, müssen die neuen Funktionsträger in ihre weisungsfreie Tätigkeit als Vermittler zwischen Behördenleitung und dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit erst einmal hineinwachsen.

Hier treten erfahrungsgemäß Situationen und Fragestellungen auf, bei denen die behördlichen Datenschutzbeauftragten in ihrer Organisationseinheit oft keine oder nur wenig fachliche Unterstützung erwarten können. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit wird daher künftig vermehrt Angebote bereitstellen, die einen vertieften Erfahrungs- und Wissensaustausch unter den behördlichen Datenschutzbeauftragten ermöglichen sollen.

Wir planen bereits ab 2010 ein umfassendes Schulungs- und Fortbildungsprogramm für alle behördlichen Datenschutzbeauftragten in Hamburg zu veranstalten. Dies richtet sich in erster Linie an die neu bestellten Kolleginnen und Kollegen, kann jedoch auch als Auffrischung und Aktualisierung des Wissens für bereits erfahrene Datenschutzbeauftragte genutzt werden.

Gleichzeitig bieten wir an, durch halbjährliche Treffen die Kontakte zwischen den Datenschutzbeauftragten zum gemeinsamen Erfahrungsaustausch zu intensivieren. Dadurch sollen gerade neu berufene Kolleginnen und Kollegen Unterstützung und Kontakte finden. Parallel hierzu werden wir die Errichtung eines SharePoints für eine schnelle und serviceorientierte Kommunikationsplattform zwischen den Datenschutzbeauftragten ermöglichen.

Insgesamt werden damit unterschiedliche Kooperations- und Kommunikationsangebote bereitgestellt, die die behördlichen Datenschutzbeauftragten bei der eigenverantwortlichen Erfüllung ihrer Aufgaben künftig unterstützen werden.

3.3 Modul 3 – Präventive Kontrollverantwortlichkeit

Neben dem zuvor erwähnten Modul des Selbstdatenschutzes und dem auf Freiwilligkeit basierenden Instrument der regulierten Selbstregulierung kommt schließlich auch der klassischen, unmittelbaren Verhaltenssteuerung durch behördliche Kontrolle und Vollzug innerhalb des Konzepts Hamburger Datenschutz 2010 eine tragende Rolle zu.

Ein präventiver, auf die Verhinderung von Datenmissbrauch und Datensicherheitsmängeln abzielender Datenschutz ist unabdingbar. Er entspricht der Schutzpflicht, die die Datenschutzbehörde sowohl für die informationelle Selbstbestimmung als auch für die Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme der Bürgerinnen und Bürger hat.

Den wichtigen Aufgaben im Vollzugs- und Überwachungsbereich wird die Dienststelle künftig im Rahmen ihrer tatsächlichen Möglichkeiten auch durch eine stärker präventiv ausgerichtete Strategie nachkommen. Dabei steht das Ziel im Vordergrund, die sich aus der Häufung individueller Eingaben ergebenden konkreten Defizite künftig zum Anlass zu nehmen, ausgedehnte anlassunabhängige Vorabkontrollen gerade in den besonders datenschutzrelevanten Bereichen wahrzunehmen.

3.3.1 Kontrollverantwortung gegenüber nicht-öffentlichen Stellen

Die Durchführung derartiger anlassunabhängiger Kontrollen von privaten Daten verarbeitenden Stellen durch die Dienstelle war im Berichtszeitraum aus unterschiedlichen Gründen zwischenzeitlich weitgehend erlahmt: Wurden im Tätigkeitszeitraum 2004/2005 immerhin 125 anlassunabhängige Prüfungen durchgeführt (vgl. 20. TB, S. 115), so sank die Zahl für 2006 auf 26, für 2007 auf lediglich 6 und für 2008 auf 21 Prüfungen. Ab dem 2. Halbjahr 2009 stieg die Zahl der anlassfreien Prüfungen auf 32 weiter an, ohne jedoch auch nur ansatzweise das Niveau zu erreichen, das für eine wirksame präventive Kontrolle der Unternehmen erforderlich wäre.

Wir planen, das Konzept anlassunabhängiger Prüfungen mit dem Modul einer eigenverantwortlichen Steuerung unmittelbar zu vernetzen und die Anzahl der Prüfungen für den nächsten Berichtszeitraum erheblich zu steigern. Das Ziel, die betrieblichen Datenschutzbeauftragten mehr in die Eingabenbearbeitung im Rahmen eines „Vorverfahrens" einzubeziehen, legt es insoweit nahe, zunächst eine übergreifende Kontrolle der Erfüllung der gesetzlichen Pflicht zur Bestellung von betrieblichen Datenschutzbeauftragten bei Hamburger Unternehmen vorzunehmen. Im Rahmen der letzten größeren Kontrolle im Zeitraum 2004-2005 hatten immerhin 20 % der geprüften Firmen keine Datenschutzbeauftragten bestellt (20. TB, S. 120). Ausweislich der Prüfungen im Berichtszeitraum 2008/2009 waren von 56

geprüften Unternehmen 25 zur Bestellung eines betrieblichen Datenschutzbeauftragten verpflichtet. In 13 Fällen blieb eine Bestellung aus. Folglich waren sogar über 50 % aller von uns geprüften Betriebe ihrer Verpflichtung nach dem BDSG nicht nachgekommen (22. TB, 11.2).

Die Zahlen verdeutlichen die Notwendigkeit einer begleitenden anlassunabhängigen Kontrolle. Es ist davon auszugehen, dass bereits die Ankündigung einer flächendeckenden Kontrolle die Unternehmen künftig zur Bestellung betrieblicher Datenschutzbeauftragter in stärkerem Maße motiviert. Mittel- bis langfristig sollte dadurch auch eine Entlastung unserer Dienststelle im Bereich der Eingabenbearbeitung möglich werden. Kontrollen der gesetzlichen Pflicht zur Bestellung von Datenschutzbeauftragten werden die Unternehmen dazu bewegen, stärker ihre Kompetenz zur eigenverantwortlichen Organisation des Datenschutzmanagements wahrzunehmen.

Um eine möglichst breite, branchenorientierte anlassunabhängige Prüfung mit hoher Effizienz zu erreichen, haben wir ein schriftliches Prüfungskonzept erarbeitet. Dessen Umsetzung soll die Bedeutung der Datenschutzbeauftragten in den Unternehmen stärken und dort, wo trotz gesetzlicher Verpflichtung keine betrieblichen Datenschutzbeauftragten benannt sind, deren zeitnahe Bestellung erwirken. Ab Januar 2010 werden daher in verschiedenen Phasen jeweils datenverarbeitende Betriebe aus bestimmten Branchen angeschrieben und gebeten, einen Fragebogen zur Bestellung von betrieblichen Datenschutzbeauftragten auszufüllen und an uns zurückzusenden. Nach Maßgabe der Auswertung sind sodann weitere konkrete Prüfungsschritte einzuleiten.

Das schriftliche und anlassfreie Prüfungskonzept beschränkt die Prüfungstätigkeit zunächst auf den Versand der Schreiben und die Kontrolle des Eingangs und des Inhalts der Antworten der Unternehmen: Es steigert die Wahrscheinlichkeit für Hamburger Firmen, Ziel einer Prüfungsanfrage zu werden. Eine Zunahme der Prüfungen sollte das Bewusstsein für den Datenschutz in Hamburger Unternehmen künftig stärken.

Das schriftliche Prüfungskonzept kann dann im weiteren Verlauf schrittweise auf besonders datenschutzsensible Bereiche ausgedehnt werden. Das gilt gerade vor dem Hintergrund, dass das BDSG zahlreiche neue Vorschriften über Adresshandel, Auskunfteien, den Arbeitnehmerdatenschutz und zum Scoring enthält.

Anlassunabhängige Prüfungen, die von Informationsangeboten der Dienststelle über die neuen rechtlichen Anforderungen flankiert werden, könnten dazu beitragen, den Vollzug der neuen Regelungen zu optimieren. Mit diesem Instrument ließe sich dann auch dem Bereich der stetig wachsenden Videoüberwachung durch nicht-öffentliche Stellen begegnen.

3.3.2 Kontrollverantwortung gegenüber öffentlichen Stellen

Auch im öffentlichen Bereich wird angestrebt, künftig in verstärktem Maße anlassunabhängige Prüfungen durchzuführen. Dies gilt gerade dort, wo eine verlässliche interne Kontroll- und Kommunikationsstruktur bislang durch behördliche Datenschutzbeauftragte nicht garantiert wird.

Übergreifend kontrollrelevant ist der Bereich der Videoüberwachung durch öffentliche Stellen der Freien und Hansestadt Hamburg, bei der wir jüngst die Schaffung einer verfassungsrechtlich erforderlichen gesetzlichen Ermächtigungsgrundlage

gefordert hatten (dazu s. unter III. 1.2). Wir werden die Umsetzung der neuen Vorschriften begleiten, gerade auch gegenüber bereits vorhandenen Videokameras.

Im öffentlichen Bereich sind überschneidende, für alle öffentlichen Stellen gleichsam bestehende Probleme des Datenschutzes nur in geringem Umfang vorhanden. Deshalb sind vornehmlich Ansätze für einzelne Spezialbereiche zu entwickeln.

Grundsätzlich gilt: Wir sind bestrebt, unsere Kontrollverantwortung gegenüber den Behörden mehr als bisher gerade in den Bereichen wahrzunehmen, in denen eine auf Kooperation und Kommunikation ausgerichtete Zusammenarbeit mit den öffentlichen Stellen bislang noch nicht oder nur unzureichend hergestellt werden konnte. Dabei kommt dem Kriterium der Bestellung von behördlichen Datenschutzbeauftragten eine zentrale Bedeutung zu.

4. Ausblick

Das mit den beschriebenen Modulen verbundene Konzept Hamburger Datenschutz 2010 wird schrittweise in die Dienstelle integriert. Einer schnellen Umsetzung steht nicht zuletzt das Erfordernis der zuverlässigen Erfüllung der bisherigen Aufgabenschwerpunkte der Dienststelle entgegen. Das Konzept zielt auf eine kontinuierliche Umsetzung und damit auf eine mittelfristige Wirksamkeit. Wir werden uns die nötige Zeit nehmen, um die neuen Instrumente und Maßnahmen zu evaluieren und sie – wenn nötig – den praktischen Gegebenheiten anzupassen.

Das Konzept Hamburger Datenschutz 2010 markiert insoweit einen ersten wichtigen Schritt zur Neuausrichtung der Dienststelle. Wir werden über die weiteren Phasen der Implementierung der neuen Instrumente berichten.

II. INFORMATIONS- UND KOMMUNIKATIONSTECHNIK

1. FHHportal

Bei der Verarbeitung von sensiblen personenbezogenen Daten sind zusätzliche technische Maßnahmen erforderlich.

Das FHHportal ist eine webbasierte Plattform zur Präsentation von Informationen und zur Zusammenarbeit von Beschäftigten der FHH. Es bietet einen zentralen Zugang zu zahlreichen Arbeitsbereichen, die durch Behörden, Ämter, Projekt- oder andere Teams aufgebaut und genutzt werden können.

Die technologische Basis bildet die Microsoft Office SharePoint-Technologie, mit der ein umfangreicher Werkzeugkasten bereitgestellt wird und keine fertige Lösung. So bietet das FHHportal Dokumentenmanagementfunktionen wie Versionierung, die Strukturierung über Metadaten sowie eine bedarfsgerechte Anzeige von so genannten Dokumentbibliotheken und Listen in verschiedenen Ansichten. Mit diesem FHHportal steht damit eine Infrastruktur zur Verfügung, deren Funktionalität deutlich über den File-Service und den Einsatz gemeinsamer Laufwerke hinausgeht.

Die jeweilige Stelle, die einen Bereich im FHHportal einrichten möchte, muss die bereitzustellenden Informationen strukturieren und auch sicherstellen, dass nur zugriffsberechtigte Personen diese Informationen einsehen können. Dazu steht eine Rechteverwaltung des FHHportals zur Verfügung. Bereits im 21. TB, 2.8

haben wir die Anforderungen dargestellt, die zu beachten sind, wenn personenbezogene Daten im FHHportal verarbeitet werden sollen.

Die Finanzbehörde, bei der die Fachliche Leitstelle des FHHportals angeordnet ist, hat im Berichtszeitraum eine Richtlinie zur Nutzung des FHHportals erlassen, die verbindliche Vorgaben für alle Nutzer macht. Danach dürfen personenbezogene Daten im FHHportal bereitgestellt werden, wenn sichergestellt ist, dass nur Nutzer von derjenigen Daten verarbeitenden Stelle auf die Daten zugreifen können, aus der die Daten stammen. Andernfalls muss die Stelle vor der Bereitstellung der Daten prüfen, ob die Voraussetzungen des automatisierten Abrufes bzw. gemeinsamen Nutzung, die das HmbDSG festschreibt, erfüllt sind. In einer ergänzenden Risikobetrachtung ist insbesondere bei sensiblen personenbezogenen Daten von der Stelle auch festzulegen,

- welcher Schutzbedarf besteht,
- ob lesende Zugriffe zu protokollieren sind und wenn ja, festzuschreiben, wer die Protokolle unter welchen Bedingungen auswertet und wann die Protokolle zu löschen sind,
- ob spezielle Zugriffsbeschränkung erforderlich sind und
- dass die Daten nicht für eine Volltextrecherche indexiert werden.

Die Fachliche Leitstelle hat die im 21. TB erhobene Forderung aufgegriffen, so dass eine übersichtlichere Darstellung der eingestellten Zugriffsregelungen ermöglicht wird. Die Fachliche Leitstelle will zusätzliche die anwendenden Stellen durch weitere Einführungshinweise unterstützen, so dass die datenschutzrechtlichen Anforderungen einfacher eingehalten werden können. Das Vorhaben einer technisch unterstützten Petitionsverarbeitung zeigt, dass solche Hinweise auch dringend notwendig sind. Bei diesem Verfahren, das von der Bürgerschaftskanzlei geplant wird, werden zum Teil sehr sensible Daten verarbeitet. Die Daten sollten für die weitere Bearbeitung mehreren Behörden gemeinsam zur Verfügung gestellt werden. Da jedoch keine Rechtsgrundlage für eine gemeinsame Verarbeitung besteht, konnte eine gemeinsame Nutzung nicht realisiert werden. Auch waren in der Risikoanalyse, die uns zunächst vorgelegt wurde, nicht alle erforderlichen technischen Maßnahmen zum Schutz der sensiblen Daten enthalten.

2. IT-Planungsrat – Datenschutz darf nicht auf der Strecke bleiben

Die Datenschutzbeauftragten der Länder müssen im IT-Planungsrat vertreten sein.

Eine sichere und effektive öffentliche Informationstechnologie bildet das Rückgrat der öffentlichen Verwaltung von Bund und Ländern. Durch das E-Government steigen die Anforderungen an eine sichere IT-Unterstützung kontinuierlich. Dafür sind verlässliche und sichere Netze für den Austausch zwischen Bund und Ländern eine unverzichtbare Voraussetzung. Die gemeinsame Festlegung von einheitlich anzuwendenden Standards kann dazu beitragen, einen effizienten, schnellen und sicheren Datenaustausch zu ermöglichen. Mit der Möglichkeit der Zusammenarbeit von Bund und Ländern und der Länder untereinander, informationstechnische Systeme gemeinsam zu betreiben und auch gemeinsame Institutionen zu errichten, soll ein Rahmen geschaffen werden, in dem angemessen und zeitnah auf die Anforderungen reagiert werden kann. Dazu soll ein zentraler, hochrangig besetzter IT-Planungsrat von Bund und Ländern eingerichtet werden, der diese Zusammenarbeit steuert.

Die Rechtsgrundlage für den Planungsrat soll durch einen Staatsvertrag geschaffen werden. Wir haben schon sehr frühzeitig aufgezeigt, dass die Verlagerung von Steuerungs- und Verantwortungsfunktion der parlamentarischen Gesetzgeber in Bund und Ländern durch den Staatsvertrag auf den IT-Planungsrat verfassungsrechtlich bedenklich ist, da mit dem IT-Planungsrat auf Vollzugsebene ein Mischgremium von Bund und Ländern geschaffen wird, das künftig die wesentlichen Vorgaben für die Planung und Errichtung informationstechnischer Systeme setzen wird. Die Regelungen im vorgesehenen Staatsvertrag gehen dabei teilweise über die Ermächtigungsnorm des Art. 91c Grundgesetz hinaus.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung darauf hingewiesen, dass die informationstechnische Kooperation von Bundes- und Landesbehörden zunehmend die Verarbeitung von personenbezogenen Daten betrifft, die durch technische und organisatorische Maßnahmen vor Missbrauch zu schützen sind, etwa durch wirksame Verschlüsselungsverfahren.

Das Bundesverfassungsgericht hat die besondere Bedeutung der informationellen Selbstbestimmung und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für den Schutz des Persönlichkeitsrechts hervorgehoben. Der in einem Staatsvertrag vorgesehene IT-Planungsrat muss diesen Vorgaben bei der Festlegung verbindlicher Interoperabilitäts- und IT-Sicherheitsstandards für die Datenverarbeitung Rechnung tragen. Für Entscheidungen in grundrechtssensiblen Fragestellungen muss auch der IT-Planungsrat die Zuständigkeit der Parlamente in Bund und Ländern berücksichtigen. Die im Staatsvertrag vorgesehene vorrangige Verwendung bestehender Marktstandards darf nicht dazu führen, dass Verfahren ohne angemessenen Datenschutz beschlossen werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat es begrüßt, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an den Sitzungen des IT-Planungsrats teilnehmen soll. Sie hält es jedoch für geboten, auch die Landesdatenschutzbeauftragten einzubeziehen.

Wir setzen uns vor diesem Hintergrund nachdrücklich dafür ein, dass Hamburg seinen Einfluss geltend macht, auf eine verfassungsgemäße Ausgestaltung der Geschäftsordnung des IT-Planungsrats zu achten und die Beteiligung der Datenschutzbeauftragten der Länder zu berücksichtigen. Die Finanzbehörde hat zugesagt, dieses Anliegen aufzugreifen.

3. NGN – Voice over IP in der FHH

Die Weichen für die Einführung der Voice-over-IP-Technik in der FHH sind gestellt. Die Sicherheit darf dabei nicht auf der Strecke bleiben.

Seit 2006 befasst sich die Finanzbehörde in enger Kooperation mit Dataport mit der Planung, die Telefonie der FHH von der jetzigen auf ISDN basierenden Technik auf Voice over IP umzustellen. Voice over IP (VoIP, unscharf auch als Internettelefonie bezeichnet) basiert auf Techniken, die ursprünglich für den Transport von Daten in Computernetzwerken, insbesondere dem Internet, entwickelt wurden (20. TB, 1.8). Das Projekt NGN (Next Generation Network) ist dabei allerdings nicht auf das Internet, sondern allein auf die eigene Netzwerkinfrastruktur der FHH bezogen. Eine Nutzung der VoIP-Technik im Übergang in das öffentliche Fernsprechnetz ist nicht geplant.

Wesentliche Beweggründe für die Umstellungsplanungen sind:

- Ersatz (zukünftig) nicht mehr wirtschaftlich betreibbarer klassischer TK-Anlagen
- Technologische Vereinheitlichung
- Funktionserweiterung durch Integration von Computer- und Telefontechnik

An diesen Planungen wurden wir frühzeitig beteiligt. Der Schwerpunkt unserer Aufmerksamkeit lag dabei bei der Begleitung und der planerischen Umsetzung der Sicherheitskonzepte, die in Zusammenarbeit mit einer externen Beratungsfirma erstellt wurden. Grundlage dabei war eine enge Orientierung an der Vorgehensweise und den Empfehlungen des Bundesamt für Sicherheit in der Informationstechnik (BSI), das für den Bereich Voice over IP mittlerweile sehr detaillierte Hinweise ausgearbeitet hat.

Bei Redaktionsschluss standen noch formale Festlegungen der Lenkungsgruppe auf bestimmte Kernelemente des Sicherheitskonzepts aus. Von besonderer Bedeutung dabei ist aus unserer Sicht die Verschlüsselung des Sprachverkehrs, da auf diese Weise einer ganzen Reihe von Risiken begegnet werden kann, die durch die enge Anbindung von Telefonie und Informationstechnologie entsteht. Da das BSI eine deutliche Empfehlung für die verschlüsselte Übertragung ausspricht und die entstehenden Mehrkosten insgesamt vergleichsweise gering sind, wäre ein Verzicht auf die Verschlüsselung schwer begründbar. Zudem müssten dann auf Grundlage einer Risikoanalyse alternative Schutzmaßnahmen getroffen werden, was den Einführungsprozess vermutlich eher verzögern dürfte.

Wir werden uns daher weiter energisch dafür einsetzen, dass dieses Sicherheitselement, neben anderen, Bestandteil eines Systems wird, das für einen voraussichtlich sehr langen Zeitraum in der FHH zum Einsatz kommen wird.

4. Sicherheitsmanagement in der FHH

Die Finanzbehörde hat sich auf den Weg zu einem strukturierten Umgang mit dem Thema IT-Sicherheit gemacht. Diese Abkehr vom Prinzip der behaupteten oder gefühlten Sicherheit ist eine wesentliche Entwicklung, fordert jedoch weitere kontinuierliche Anstrengungen.

Bereits in unserem letzten Tätigkeitsbericht berichteten wir über die Aktivitäten der Finanzbehörde zur Analyse der IT-Sicherheit (vgl. 21. TB, 2.10). Diese wurden fortgesetzt durch eine Erhebung zur Grundschutzkonformität von ESARI-Clients, ebenfalls im Auftrag durchgeführt vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD).

Diese Untersuchungen lassen neben dem bereits erreichten Stand auch verschiedene Defizite erkennen:

- Die bestehenden Regelungen sind teilweise ergänzungs- und überarbeitungsbedürftig.
- Die lokale Administration der ESARI-Clients wird zu umfassend genutzt und führt zu einem nicht revisionssicheren Betrieb.
- Verschiedene technische Einstellmöglichkeiten sind zu verbessern.
- Die Transparenz für die Nutzer ist unzureichend.

Die Finanzbehörde hat dies insoweit aufgegriffen, als von Seiten der zentralen IT-Steuerung ein Maßnahmen- und Zeitplan vorgelegt wurde, der eine Beseitigung

der Defizite bis Ende 2010 vorsieht. Leider war diese Anfang des Jahres 2009 vorgelegte Planung bei Redaktionsschluss dieses Berichts in einigen Punkten bereits in Verzug. Zudem sollen zunächst vorrangig Maßnahmen getroffen werden, um ein normales Schutzniveau zu erreichen, so dass Lösungen für die Verarbeitung von Daten mit einem höheren Schutzniveau frühestens in der zweiten Hälfte des Jahres 2010 zu erwarten sind.

Allerdings wurde mittlerweile die neu geschaffene Stelle des IT-Sicherheitsmanagements in der Finanzbehörde besetzt, so dass nun eine zentrale Aufgabenwahrnehmung in diesem Bereich sichergestellt ist.

Aus unserer Sicht sind folgende Punkte vorrangig zu bewegen:

- Die Konzeption und der Aufbau eines behördenübergreifenden Sicherheitsmanagements unter Führung der Finanzbehörde.
- Die Verankerung einer entsprechenden IT-Sicherheitsleitlinie im politischen Raum (Senat).
- Die Entwicklung solcher Maßnahmen, die ergänzend bei einem höheren Schutzbedarf ergriffen werden können.

Insgesamt ist die Bereitschaft der Finanzbehörde, sich dem komplexen Thema der IT-Sicherheit aus einer einheitlichen Gesamtperspektive zu widmen, zu begrüßen. Eine stärkere, insbesondere auch formale Orientierung an Standards wie dem BSI-Grundschutz ist dabei aus unserer Sicht allerdings bereits deshalb geboten, da entsprechende Verpflichtungen in einzelnen Bereichen schon jetzt bestehen und im Zuge nationaler und europäischer Vorgaben vermehrt auf die FHH zukommmen werden (siehe z.B. II 2.).

5. Videoüberwachungstechnik

Videoüberwachung durch öffentliche Stellen muss immer auf eine ausdrückliche Rechtsvorschrift gestützt sein. Die technische Ausgestaltung muss sich an den datenschutzrechtlichen Grundsätzen orientieren. In Abhängigkeit von den Leistungsmerkmalen der eingesetzten Technik kann dies vielfältige technische und organisatorische Maßnahmen erfordern.

Videotechnik hat Einzug in viele private Lebensbereiche erhalten. So werden mit Hilfe von Camcordern ganz selbstverständlich Urlaubserinnerungen und mit dem Foto-Handy Alltagssituationen festgehalten. Das Videorückfahrtsystem hilft beim Einparken, das Video-Babyfon beim Babysitten.

Videotechnik ist allgegenwärtig und allgemein verfügbar. Sie ist letztlich in allen Preisklassen mit unterschiedlichstem Funktionsumfang erhältlich. Mit immer kleineren Kameras, verbunden mit noch kleineren Speichermedien mit hoher Speicherkapazität, kann jede Lebenssituation mühelos in Bild und Ton detailgetreu aufgezeichnet, aufgearbeitet und genutzt werden.

Die Entwicklung in der Videotechnik orientiert sich grundsätzlich an Zielen wie der besten Bild- und Klangqualität, der Handhabbarkeit der Geräte usw. Sie ist nicht an datenschutzrechtlichen Grundsätzen wie denen der Datensparsamkeit und -vermeidung ausgerichtet. Dies ist insbesondere dann zu beachten, wenn Videotechnik nicht ausschließlich für persönliche oder familiäre Zwecke genutzt wird, son-

dern öffentliche Stellen diese im Rahmen eines Videoüberwachungssystems einsetzen.

Die Überwachung öffentlich zugänglicher Bereiche mittels eines Videoüberwachungssystems beinhaltet in der Regel die Verarbeitung personenbezogener Daten. Im Gegensatz zu sonstigen Verfahren ist die Datenverarbeitung bei Einsatz von Videotechnik grundsätzlich nicht auf einzelne, erforderliche Informationen (vordefinierte Datenfelder) beschränkbar. Sie erfasst vielmehr sämtliche visuell wahrnehmbare Daten wie Aufenthaltsort und -zeit, Gesicht und Mimik, Frisur/Kopfbedeckung, Art und Zustand der Kleidung, Gepäck, optisch erkennbarer Allgemeinzustand, Kontakt- und Begleitpersonen, Verhalten allein und in der Gruppe, usw. Es werden Daten kompletter Lebenssituationen von Personen erhoben, die in der Regel nichts weiter verbindet, als dass sie den gleichen öffentlichen Raum zum ganz überwiegenden Teil für zulässige Zwecke nutzen.

Die Verarbeitung personenbezogener Daten sowie die Beobachtung öffentlich zugänglicher Bereiche mit Hilfe von Videoüberwachungssystemen müssen daher immer auf eine ausdrückliche Rechtsvorschrift gestützt sein. Während in datenschutzrechtlichen Bestimmungen über die Zulässigkeit der Verarbeitung personenbezogener Daten in der Regel auf die zu verarbeitenden Daten abgestellt wird, wird diese Systematik bei Regelungen zur Videoüberwachung vielfach dahingehend durchbrochen, dass für definierte Zwecke nicht die Verarbeitung bestimmter Daten, sondern die Nutzung von optisch-elektronischen Einrichtungen – also einer bestimmten Technik – zugelassen wird.

Dies bedeutet jedoch nicht, dass jedes handelsübliche Gerät ohne weiteres zur Überwachung genutzt werden darf/sollte. In der Regel wird vielmehr eine Vielzahl flankierender, technischer und organisatorischer Maßnahmen notwendig sein, um den allgemeinen datenschutzrechtlichen Grundsätzen und datenschutzrechtlichen Bestimmungen zu genügen.

Dies sollte bereits bei der Beschaffung, insbesondere jedoch bei der Installation der einzelnen Systemkomponenten und dem Betrieb der Anlage berücksichtigt werden. Sämtliche Funktionalitäten der Einzelkomponenten sollten auf die Erforderlichkeit im Hinblick auf den definierten Zweck der Anlage kritisch hinterfragt und die Anlage auf erforderliche Funktionen beschränkt werden. Überflüssige Funktionen bergen häufig zusätzliche Risiken für die Rechte der Betroffenen. Von einem Einsatz sollte daher abgesehen werden.

Einige Beispiele:

- Handelsübliche Videoüberwachungskameras verfügen vielfach über Audiofunktionen und damit grundsätzlich über die Möglichkeit der akustischen Raumüberwachung und/oder der Tonaufzeichnung. Die Erfassung von Begleitton ist zur Zielerreichung meist nicht erforderlich und stellt einen erheblichen Eingriff in die Privatsphäre der Betroffenen dar. Zudem stellt § 201 StGB die unbefugte Aufnahme des nichtöffentlich gesprochenen Wortes, die Nutzung einer solchen Aufnahme, das Abhören mit einem Abhörgerät ebenso unter Strafe wie einen entsprechenden Versuch.

Wenn keine spezialgesetzliche Befugnis für Abhörmaßnahmen oder Tonaufzeichnungen vorliegt, dürfen Geräte daher nur ohne Audiofunktionalitäten zum Einsatz kommen. Einige Hersteller stellen daher bereits eine Funktion zur irreversiblen Zerstörung der Audiofunktion bereit.

- Wesentlich für die Zulässigkeit einer Videoüberwachungsmaßnahme ist der mögliche und tatsächliche Aufnahmebereich der Kameras. Bereiche, die aus rechtlichen Gründen von einer Überwachung ausgenommen werden müssen, dürfen nicht beobachtet werden. Die räumliche und zeitliche Ausdehnung der Videoüberwachung ist zudem auf das für den Zweck der Anlage erforderliche Maß zu beschränken.

Durch geeignete technische und organisatorische Maßnahmen muss gewährleistet werden, dass der Aufnahmebereich tatsächlich auf das rechtlich zulässige Maß beschränkt wird. Dies kann feste Kameraeinstellungen in Verbindung mit der Nutzung von Funktionen wie dem privat-masking (Definition von Privatbereichen) erfordern. Durch Reduzierung des Blickwinkels der Kamera, Verzicht auf Aufzeichnung oder Beschränkung der Aufnahmezeiten, verkürzte Speicherzeiten sowie den Einsatz existierender technischer Möglichkeiten wie der Verschleierung (verpixeln) von Video-Klardaten in Echtzeit können Daten zudem erheblich reduziert werden.

Es muss sichergestellt werden, dass ein rechtlich zulässiger Aufnahmebereich nicht durch unbefugte Änderung der Einstellungen und der Ausrichtung der Kameras in unzulässiger Weise verändert wird. Dies beinhaltet gegebenenfalls den Verzicht auf oder die besondere Reglementierung von Fernsteuerungsfunktionen, Vandalismusschutz für die Kamera, Zugangs- und Zugriffsbeschränkungen zur Anlage.

- Übersichtsaufnahmen, auf denen Personen oder sonstige personenbeziehbare Kennzeichen nicht erkennbar scheinen, werden häufig als datenschutzrechtlich unkritisch angesehen.

Viele digitale Kameras verfügen jedoch inzwischen über eine sehr hohe Bildauflösung. Damit können auch bei Übersichtsaufnahmen viele Details erfasst werden, die nachträglich erheblich vergrößert und damit personenbeziehbar werden können.

Geräte mit besonderen Leistungsmerkmalen (z.B. besonders hohe Bildauflösung, Nachtsicht, Zoom, Fernsteuerung) sollten daher nur zum Einsatz kommen, soweit sie für den Zweck der Anlage erforderlich sind.

- Die Daten müssen während des gesamten Verarbeitungsprozesses (Aufnahmegerät, Netz, Speichermedien, etc.) bis zur Löschung sicher vor Einsichtnahme durch Dritte geschützt sein.

Die (sichtbaren) Kameras liefern zumeist nur die Bilder. Die weitere Verarbeitung erfolgt nachgeordnet über einen Monitor, auf einem Videorekorder oder einem zentralen PC/Server mit Video-Management-Software. Die verschiedenen Systemkomponenten sollten möglichst in einem geschlossenen Netz betrieben und nicht mit anderen Netzen (Internet, Verwaltungsnetz etc.) verbunden werden. Eine separate Verkabelung der Kameras bis zum zentralen Aufnahmegerät bedeutet Aufwand, minimiert jedoch die Möglichkeiten eines Zugriffs/Angriffs von außen. Jede Netzverbindung birgt potenziell Gefahren unberechtigter Zugriffe und stellt hohe Anforderungen an eine sichere Konfiguration. Ist beispielsweise eine Netzwerkkamera mit Verbindung zum Internet fehlerhaft konfiguriert, sind die Daten gegebenenfalls weltweit einsehbar.

- Werden Kameras über drahtlose Technik eingebunden, so muss gewährleistet werden, dass die Daten nur von den eigenen Geräten empfangen werden und nicht auf den Empfangsgeräten Dritter zur Ansicht kommen. Dies kann nur aus-

geschlossen werden, wenn entsprechende Schutzmaßnahmen getroffen werden. Eine Übertragung der Daten sollte daher insbesondere bei drahtloser Technik nur verschlüsselt erfolgen.

- Die Daten der Kameras werden in der Regel auf einem zentralen Aufnahmegerät zusammengeführt. Das Aufnahmegerät ist ebenfalls vor Fremdzugriffen zu schützen (Zugangsschutz, Zugriffsschutz durch Berechtigungsvergabe, Zugriffsprotokollierung).

Ein zusätzlicher Schutz kann durch eine verschlüsselte Speicherung erreicht werden.

- Die Weiterverarbeitungs-, Analyse-, Auswertungs- aber auch Veränderungsmöglichkeiten von Videoaufzeichnungen sind vielfältig. Der Glaube an das „mit eigenen Augen gesehene" – und damit die Beweiskraft von Bildaufnahmen – ist gemeinhin stark.

Zum Schutz der Betroffenen müssen Maßnahmen getroffen werden, die geeignet sind, zu gewährleisten, dass nur Befugte die personenbezogenen Daten zur Kenntnis nehmen können und festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.

Vor der Inbetriebnahme der Anlage sollte festgelegt werden, welchen Personen für welche Aufgaben unter welchen Voraussetzungen und auf welchen Wegen welche Zugriffsmöglichkeiten eingeräumt werden müssen und wie dies gewährleistet und überprüft werden kann (Berechtigungsverwaltung, Zugriffsprotokollierung, Diebstahlsicherung etc.).

- Bei der Weitergabe sind die rechtlichen Grenzen der Übermittlungsbefugnis zu beachten.

Ist die Weitergabe/Übergabe von Daten etwa an Strafverfolgungsbehörden erforderlich, so muss hierfür sowohl organisatorisch als auch technisch ein geregeltes Verfahren geschaffen werden.

- Personenbezogene Daten unterliegen der Zweckbindung, d.h. sie dürfen grundsätzlich nur für die Zwecke verarbeitet werden, für die sie erhoben wurden. Sie sind zu löschen, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die Daten verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Je nach Installation werden die Daten im internen Speicher der Kamera, einem Videorecorder, auf einem Server o.ä. gespeichert. Die Löschverpflichtung bezieht sich auf die Daten. Das Löschkonzept muss daher sämtliche Speichermedien einbeziehen.
- Häufig werden Kameras eingesetzt, welche als solche gar nicht wahrgenommen werden. Sind diese Kameras als solche ausfindig gemacht, ist für den Betroffenen noch lange nicht ersichtlich, wann er sich im Aufnahmebereich befindet und ob er tatsächlich beobachtet oder gar aufgezeichnet wird.

Für die Betroffenen muss jedoch erkennbar sein, dass sie sich in einem videoüberwachten Bereich bewegen (Kennzeichnung).

6. Hamburger Informationsmanagement

Die Einführung moderner Hilfsmittel zur Arbeitsunterstützung bergen häufig auch Gefahren für die Rechte Betroffener.

Im Februar 2008 wurde in der Finanzbehörde das Projekt Hamburger Informationsmanagement (HIM) eingesetzt. Ziel des Projektes ist die Schaffung eines einheitlichen elektronischen Dokumentenmanagementsystems in der hamburgischen Verwaltung. Dies umfasst die Einführung einer Plattform für elektronische Entscheidungsvorgänge (HIM-Workflow-Komponente) als Voraussetzung für eine medienbruchfreie Vorgangsbearbeitung ebenso wie die einer systemübergreifenden elektronischen Suche mittels Volltextrecherche (Komponente HIM-Suche). Die Anbindung an die elektronische Aktenverwaltung und -archivierung (ELDORADO) ist hierbei vorgesehen.

Es wurden frühzeitig Gespräche mit uns aufgenommen, in welchen insbesondere die datenschutzrechtliche Problematik der HIM-Suchfunktion erörtert wurde, da diese Komponente vorrangig eingeführt werden soll.

Die Suchfunktionalität innerhalb des Projekts HIM soll die Arbeit durch die Möglichkeit unterstützen und vereinfachen, Informationen auf zentralen Datenspeichern der FHH zu finden, ohne die verschiedenen Datenquellen (FHHportal, Intranet, Exchange, Filesystem der Behörden, Gruppen- und Homelaufwerk, elektronische Akten des Dokumentenverwaltungssystems ELDORADO etc.) einzeln durchsuchen zu müssen.

Die HIM-Suche ist als Volltextrecherchesystem konzipiert. Sie erfolgt über einen zentralen Index, welcher aus der Datenbasis erstellt wird. Die Trefferlisten werden nach den Benutzerrechten des jeweils angemeldeten Benutzers gefiltert. Die Anzeige wird auf die Daten beschränkt, für die der/die Suchende zumindest lesende Berechtigung besitzt. Der Zugriff auf die gefundenen Dokumente ist durch die im Quellsystem eingerichteten Rechte reglementiert.

Die Eröffnung der Möglichkeit einer Volltextrecherche wird häufig lediglich als ein Hilfsmittel zur Arbeitsunterstützung dargestellt und verstanden. Mit der Volltextrecherche können jedoch Informationen ohne viel Aufwand selbst aus großen Mengen von unstrukturierten Texten/Dateien schnell aufgefunden werden.

Wenn die Datenbasis personenbezogene Daten beinhaltet, können mit entsprechend freien und komfortablen Auswertungsmöglichkeiten erhebliche Gefahren für die Rechte der Betroffenen verbunden sein.

Die verschiedenen Datenquellen auf den zentralen Datenspeichern der FHH enthalten immer personenbezogene Daten von Mitarbeitern als Bearbeiter. Zudem können personenbezogene Daten von Bürgern (und Mitarbeitern) als Antragsteller, Beschwerdeführer, Zuwendungsempfänger usw. in unterschiedlicher Sensibilität enthalten sein. Personenbezogene Daten dürfen nicht beliebig verarbeitet und ausgewertet werden, bei ihrer Verarbeitung ist das Zweckbindungsgebot zu beachten. Volltextrecherche kann jedoch grundsätzlich nicht auf fachbezogene, rechtlich zulässige Verarbeitungsschritte nach festgelegten Ordnungskriterien begrenzt werden. Eine nachträgliche Kontrolle erfolgter Auswertungen wäre nur mit einer umfassenden Zugriffsprotokollierung möglich.

Eine weitere Gefahr der Volltextrecherche besteht darin, dass aufgrund der Auswahl fehlerhafter Suchkriterien oder der Verwendung von Synonymen die für die Bearbeitung erforderlichen Unterlagen gegebenenfalls nicht vollständig erfasst werden – dafür aber Unterlagen in die Trefferliste aufgenommen werden, die für die Bearbeitung völlig unerheblich sind. Bei personenbezogenen Unterlagen liegt hierin eine Verletzung des informationellen Selbstbestimmungsrechts.

Die Daten verarbeitenden Stellen müssen vor einer Einbeziehung daher genau prüfen, ob und welche Daten für die HIM-Suche indiziert werden und welche von dieser Verarbeitung ausgenommen werden müssen.

Hinsichtlich des Aufbaus eines zentralen und gemeinsamen Indexes wurde auf die Erforderlichkeiten des § 11a HmbDSG hingewiesen: Es handelt sich hier um eine gemeinsame automatisierte Datei, die einer Rechtsverordnung zur Regelung der beteiligten Stellen, der Verantwortlichkeiten und der technisch-organisatorischen Maßnahmen bedarf.

Eine abschließende datenschutzrechtliche Abstimmung des Verfahrens konnte bisher noch nicht erfolgen. Überarbeitete Unterlagen wurden seitens der Finanzbehörde für den November angekündigt. Wir werden uns weiter für eine datenschutzfreundliche Ausgestaltung des Projektes einsetzen.

7. Übernahme des IuK-Netzes der Polizei durch Dataport

Unsere Bedenken zu den realisierten Datenschutz- und Sicherheitsstandards des Dienstleisters für das Polizeinetz konnten bisher nur teilweise ausgeräumt werden, weil die Polizei Hamburg Unterlagen noch nicht in dem erforderlichen Umfang erstellt hat. Die Aufklärung ist dadurch unnötig erschwert.

Im letzten Tätigkeitsbericht (vgl. 21.TB, II 2.7) berichten wir über die Übergabe des Polizei-Netzwerks an Dataport. Die Polizei Hamburg übergab ihr vorher selbst betriebenes Netzwerk für die eingesetzte PC-Hardware an den IT-Dienstleister Dataport. Außerdem gingen zahlreiche Informations-, Auskunfts- und Vorgangsbearbeitungsverfahren der Polizei in die Betreuung von Dataport über. Es bestanden erhebliche Bedenken, ob die realisierten Datenschutz- und Datensicherheitsstandards des Dienstleisters ausreichen, um den notwendigen Schutzbedarf für das Polizeinetz zu gewährleisten.

Die Bedenken konnten bisher nur teilweise ausgeräumt werden. Dazu hat es einige Treffen mit der Polizei, aber auch mit Dataport gegeben. Neben der Darstellung der Polizei zu den Veränderungen in Ihrem Netzwerk erhielten wir auch Informationen von Dataport zu der für die Polizei realisierten „Infranet"-Lösung, die zukunftsweisend ist. Zusätzlich haben wir weitergehende Betrachtungen mit Dataport unternommen, um bessere Einblicke zu gewinnen.

Unterlagen von der Polizei liegen nur teilweise vor. Die Migration zu Dataport hat auch Auswirkungen auf die bestehenden datenschutzrechtlichen Unterlagen für die migrierten Verfahren. Der Vorschlag, die Veränderungen durch die Migration in zentralen Dokumenten abzulegen und dann mit Verweisen zu arbeiten ist zwar überlegt, aber bisher nicht realisiert worden. Unsere Empfehlung, externe Unterstützung bei der Betrachtung der Grundschutzkonformität ihrer Verfahren und zur Planung der weiteren Vorgehensweise zu nutzen, hat die Polizei zwar zur Kenntnis genommen, aber unseres Wissens bisher nicht umgesetzt.

Insgesamt hat die verspätete Beschäftigung mit diesem Themenkomplex zu mehr Arbeit, vielen Irritationen und auch verpassten Chancen geführt. Eine frühzeitige Beteiligung unserer Dienststelle und die rechtzeitige Erstellung von Dokumentation und der gesetzlich geforderten datenschutzrechtlichen Unterlagen ist nicht nur vorgeschrieben, sondern wäre auch für alle Beteiligten von Vorteil gewesen.

Wir werden weiterhin darauf drängen, dass die Polizei Hamburg die Mängel in ihrer Dokumentation behebt und versuchen, gemeinsam die Abstimmungsprozesse zu optimieren.

8. Migration der Polizei ins Active Directory

Die Unterrichtung über die beabsichtigte Migration der Polizei Hamburg hat uns nicht mit dem angemessenen zeitlichen Vorlauf für eine Bewertung erreicht. Notwendige Unterlagen lagen uns auch Monate nach der Umstellung noch nicht vor.

Auf einem Treffen mit der Polizei zur Übernahme des IuK-Netzes der Polizei durch Dataport (vgl. II 2.7) wurde uns beiläufig von dem geplanten Umstieg der Polizei Ende April 2009 in den zentralen Verzeichnisdienst der Stadt berichtet. Auf unser Drängen hin kam es dann zu einer Besprechung zwei Arbeitstage vor dem geplanten Umstieg der Polizei Hamburg. In diesem knappen Zeitraum blieb nicht zu mehr Zeit, als uns über das Vorhaben zu informieren. Eventuelle grundsätzliche Veränderungen an der Vorgehensweise, die sich hätten ergeben können, wären nicht mehr umsetzbar gewesen und hätten zu einem Abbruch der Migration geführt.

In dieser Besprechung erfuhren wir auch von Papieren der Kommission IuK-Sicherheit des Bundeskriminalamtes aus dem März 2009, die uns zur Verfügung gestellt wurden. Ein Schreiben der Kommission befasst sich mit einer Anfrage der Polizei Bremen, ob eine Integration von Teilen des Polizeinetzes in ein Landesbehördennetz mit der IT-Sicherheitspolicy für das Verbundnetzwerk der Länderpolizeien vereinbar ist. Die Stellungnahme der Kommission kommt zu dem Schluss, dass die Anforderungen aus der IT-Sicherheitspolicy derzeit nur erfüllt werden können, wenn ein eigenes Active Directory für das Polizeinetz eingerichtet und betrieben wird.

Wir baten die Polizei Hamburg dazu um Stellungnahme. Die Polizei hält eine Gefährdung des Verbundnetzes durch die in Hamburg von der Empfehlung abweichende Lösung für ausgeschlossen.

Ende April 2009 ist die Polizei Hamburg in den zentralen Verzeichnisdienst (Active Directory) der Freien und Hansestadt Hamburg bei Dataport migriert. Die von der Polizei Hamburg zu liefernden Unterlagen wurden jedoch erst kurz vor Redaktionsschluss des Tätigkeitsberichts (Mitte November 2009) geliefert. Über das weitere Verfahren zu diesem Thema müssen wir mit der Polizei Hamburg nach Auswertung der Unterlagen noch reden.

Auch hier gilt es, zukünftig eine derart späte Beteiligung unserer Dienststelle bei einer komplexen Veränderung und die langsame nachträgliche Bearbeitung zu vermeiden und durch rechtzeitige Beteiligung und Erstellung einer Dokumentation auch die Vorteile einer Zusammenarbeit mit dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zu nutzen.

9. Neues Haushaltswesen: Einheitliche Personennummer im Sozialhilfeverfahren, bei Ordnungswidrigkeiten und weiteren IT-Verfahren der FHH

Sensible personenbezogene Daten unterschiedlicher Fachverfahren werden zusammengeführt.

Das Verfahren Neues Haushaltswesen Hamburg (NHH) wird zum 1. Januar 2010 in der FHH eingeführt. Es wird dann das derzeitige SAP-Verfahren ablösen, mit dem

die FHH grundsätzlich alle ein- und ausgehenden Zahlungen verbucht. Über das Verfahren NHH werden beispielsweise Leistungen nach dem Bundesausbildungsförderungsgesetz, dem Bundessozialhilfegesetz und Zuwendungszahlungen geleistet, aber auch Buß- und Verwarngelder nach dem Ordnungswidrigkeitengesetz erhoben. Darüber hinaus umfasst das Verfahren ein nicht-personenbezogenes Data-Warehouse für Planungszwecke.

Die Fachliche Leitstelle des Projekts NHH, die alle vorbereitenden Projekttätigkeiten verantwortet, ist in der Finanzbehörde angesiedelt. Wir haben schon sehr frühzeitig auf zentrale datenschutzrechtliche Aspekte hingewiesen und wiederholt eingefordert, dass das Projekt diese in einer Risikoanalyse darstellt. Eine abschließende Version lag jedoch erst einen Monat vor dem Starttermin vor.

Grundsätzlich soll für jede natürliche und jede juristische Person, deren Buchungsdaten in NHH verarbeitet werden, nur ein Stammdatensatz angelegt werden, der mit der „Einheitlichen Geschäftspartner-Nummer" eindeutig identifiziert wird. Über die einheitlichen Geschäftspartner-Nummern werden somit Zahlungen im Verfahren NHH aus sehr unterschiedlichen Fachverfahren gebucht: Diese IT-Verfahren lassen sich vier Bereichen zuordnen:

- Zahlungen an Mitarbeiterinnen und Mitarbeiter, die durch die Rolle der FHH als Arbeitgeber bzw. Dienstherr begründet sind,
- Zahlungen an Bürgerinnen und Bürger aufgrund von Sozialleistungen und weiteren Ansprüchen wie z.B. Zuwendungen,
- Zahlungen von Bürgerinnen und Bürgern aufgrund hoheitlichem Handelns wie die der Verbuchung von Bußgeldern,
- Zahlungen aufgrund von fiskalischem Handeln der FHH wie dem Einkauf von Dienstleistungen oder Geräten.

Vorteile der einheitlichen Geschäftspartner-Nummer werden vom Projekt insbesondere in einer schlankeren und widerspruchsfreien Stammdatenverwaltung gesehen, der Verbesserung der Qualität zahlungsrelevanter Daten in den IT-Verfahren, der besseren Zuordnung von unklaren Zahlungseingängen und Irrläufern, der Reduzierung von Fehlzahlungen der Stadt an nicht Berechtigte sowie in der Tatsache, dass im Falle einer Insolvenz aufrechenbare Forderungen und Verbindlichkeiten leichter miteinander verrechnet werden können.

Wenn die Buchungen aus allen vier Bereichen über eine einheitliche Geschäftspartner-Nummer abgewickelt werden, könnten die Buchungen der verschiedenen Bereiche jedoch sehr leicht zusammengeführt und ausgewertet werden. Es wäre dann leicht und eindeutig feststellbar, welcher Sozialhilfeempfänger auch Zahlungen aufgrund von Ordnungswidrigkeiten geleistet hat. Auch wäre auf Knopfdruck eine Liste von Beschäftigten erstellbar, die Sozialleistungen erhalten. Lediglich durch die Vergabe von Zugriffsrechten soll diese Zusammenführung verhindert werden. Dabei ist zu bedenken, dass es in jedem SAP-System Rollen mit sehr umfassenden Rechten gibt, dass Berechtigungen leicht verändert und erweitert werden können und dass gerade das SAP-Berechtigungssystem derart komplex ist, dass es bei der Umsetzung sehr häufig zu fehlerhaften Einstellungen kommt.

Da die einheitliche Geschäftspartner-Nummer in allen zuliefernden IT-Verfahren gespeichert werden soll, wäre damit technisch eine wichtige Voraussetzung dafür geschaffen, dass die getrennten Datenbestände der jeweiligen Fachverfahren automatisiert miteinander verbunden und abgeglichen werden können. Da mit einem

solchen einheitlichen Merkmal in unterschiedlichsten IT-Verfahren ein umfassendes Persönlichkeitsabbild geschaffen werden kann, hat das Bundesverfassungsgericht im Volkszählungsurteil die Nutzung eines einheitlichen Personenkennzeichens verboten.

In Abwägung der datenschutzrechtlichen Ziele mit den haushaltärischen Anforderungen haben wir vorgeschlagen, zumindest die vier Bereiche dadurch voneinander zu trennen, dass vier bereichsspezifische Nummernkreise eingerichtet werden. Auf diese Weise wäre der Grundsatz der Verhältnismäßigkeit bei dem Eingriff in die Rechte der Betroffenen eher gewahrt. Trotz ausführlicher Erörterungen der Gefährdungen war das Projekt jedoch nicht bereit, über die Bildung einer von NHH vorgesehenen speziellen „Mitarbeiter-Geschäftspartner-Nummer" hinaus, mit der der erste Bereich abgetrennt wird, auch die weiteren drei Bereiche gegeneinander abzuschotten. Im Zuge der Erörterungen wurde darüber hinaus auch deutlich, dass die Nutzung der geplanten Mitarbeiter-Geschäftspartner-Nummer lediglich durch derzeit vorhandene technische Restriktionen des aktuellen Fachverfahrens Personal begründet ist, die im Zuge der geplanten Modernisierung (vgl. Ziffer III 2.1) entfallen wird.

Die anforderungsgerechte Realisierung eines sehr differenzierten Berechtigungskonzepts erhält unter diesen Bedingungen eine noch größere Bedeutung. Zusätzlich muss bedacht werden, dass die Buchungen der FHH zukünftig in nur einem SAP-Buchungskreis durchgeführt werden sollen. Damit wird die bisherige Trennung in verschiedene Buchungskreise aufgegeben, mit denen die Daten unterschiedlicher Behörden voneinander abgegrenzt wurden. Auch hier erfolgt der Zugriffsschutz alleine durch das Rollen- und Berechtigungssystem. Vor diesem Hintergrund und den Erfahrungen aus anderen SAP-Verfahren haben wir darauf gedrungen, bereits vor der Inbetriebnahme das realisierte Berechtigungssystem systematisch und umfassend zu prüfen. Aufgrund der Komplexität belegen alle Erfahrungen, dass dies toolgestützt erfolgen sollte. Auch auf diesen Vorschlag ist das Projekt nicht eingegangen, obwohl entsprechendes Know-How beim Dienstleister Dataport vorhanden ist.

III. DATENSCHUTZ IM ÖFFENTLICHEN BEREICH

1. Grundsatzfragen

1.1 Behördliche Datenschutzbeauftragte

Nach § 10a Abs. 1 HmbDSG ist es in das Ermessen der Daten verarbeitenden Stelle gestellt, ob sie behördliche Datenschutzbeauftragte bestellt oder nicht. Diese Bestimmung soll nach den Erläuterungen zum Gesetzestext eine flexible, an den jeweiligen Bedürfnissen und Problemen der Daten verarbeitenden Stelle orientierte Handhabung ermöglichen.

Diese Vorstellung erweist sich jedoch angesichts der zunehmenden Verbreitung des Einsatzes elektronischer Datenverarbeitungssysteme als überholt. „Inseln" einzelner Verwaltungseinheiten, für die es entbehrlich wäre, behördliche Datenschutzbeauftragte zu bestellen, sind heute nicht mehr vorhanden. Die Mehrzahl der Länder hat dem bereits Rechnung getragen und die Bestellung behördlicher Datenschutzbeauftragter gesetzlich vorgeschrieben. Hamburg sollte, wie bereits im 21. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten unter Tz. 3 gefordert, diesem Beispiel folgen. Denn ohne eine gesetzliche Verpflichtung dro-

hen notwendige Bestellungen von behördlichen Datenschutzbeauftragten an Ressourcenfragen zu scheitern.

Der Senat hat mit Beschluss vom 28.10.2008 die Finanzbehörde und die Justizbehörde beauftragt, unter Beteiligung der übrigen Behörden und Ämter ein Konzept für die Bestellung von behördlichen Datenschutzbeauftragten zu entwickeln, das die mit dem Amt verbundenen Aufgaben und Befugnisse dieser Institution, ihr Verhältnis zu den mit Datenschutzfragen befassten Linienfunktionen in der Dienststelle und ihre organisatorische Anbindung konkretisiert sowie auf die mit dieser Funktion verbundenen Kosten eingeht. Ein entsprechender Entwurf ist im November 2008 in die Behördenabstimmung gegeben worden. Der HmbBfDI wurde beteiligt. Im Dezember 2009 erhielt der HmbBfDI auf Nachfrage bei den federführenden Behörden die Auskunft, dass der Senat wegen eines noch bestehenden Dissenses derzeit nicht befasst werden könne. Streitig sei die Frage, ob und inwieweit den Daten verarbeitenden Stellen auferlegt werden solle, den durch die Bestellung behördlicher Datenschutzbeauftragter entstehenden personellen und organisatorischen Mehrbedarf jeweils aus dem Bestand der Daten verarbeitenden Stelle zu leisten.

In Einzelfällen hat diese ungeklärte Sachlage Behörden dazu veranlasst, die Bestellung behördlicher Datenschutzbeauftragter bis zur Senatsentscheidung über die Kostenfrage zurückzustellen.

Aus unserer Sicht spricht die zögerliche Haltung für die Einführung einer gesetzlichen Verpflichtung zur Bestellung von behördlichen Datenschutzbeauftragten. Unsere Erfahrung mit den behördlichen Datenschutzbeauftragten belegt, dass diese deutlich zu einer Stärkung des Datenschutzes und der Kommunikation mit dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit beitragen. Wir begrüßen daher, dass fünf von neun Fachbehörden, das Personalamt und der Rechnungshof von dem Instrument der eigenverantwortlichen Selbststeuerung Gebrauch gemacht haben. Der HmbBfDI ist diesem Beispiel gefolgt und hat Mitte 2009 einen eigenen behördlichen Datenschutzbeauftragten eingesetzt.

Leider haben sich weder die Behörde für Inneres noch die Finanzbehörde zu der Bestellung einer oder eines behördlichen Datenschutzbeauftragten entschließen können. Das ist umso bedauerlicher, als beide Behörden in ganz erheblicher Weise, die Finanzbehörde auch als Steuerungseinheit, mit Fragen des Datenschutzes und der Datensicherheit befasst sind. Im Falle einer nicht erfolgten Bestellung einer oder eines behördlichen Datenschutzbeauftragten übernimmt der HmbBfDI von Gesetzes wegen deren oder dessen Aufgaben (§ 8 Abs. 4 Satz 3 und § 9 Abs. 3 Satz 1 HmbDSG). Darin liegt jedoch kein wünschenswerter Effekt, da allein die behördlichen Datenschutzbeauftragten über die zur Erfüllung ihrer Aufgaben (§ 10a Abs. 5 in Verbindung mit § 9 und § 8 Abs. 4 HmbDSG) notwendigen internen Kenntnisse und Erfahrungen verfügen und ihre Dienststelle entsprechend fachgerecht beraten können. Der HmbBfDI kennt seiner übergreifenden Aufgabenstellung wegen nicht die datenschutzspezifischen Interna der einzelnen Daten verarbeitenden Stellen.

Ausweislich des Konzepts Hamburger Datenschutz 2010 und des dazu entwickelten Kooperationsmodells werden wir den kritischen Dialog weiter führen und die betroffenen Behörden versuchen, davon zu überzeugen, dass das Modell der behördlichen Eigenverantwortung und Selbststeuerung einer externen Kontrolle und

Überwachung durch den Hamburgischen Beauftragen für Datenschutz und Informationsfreiheit gegenüber vorzugswürdig ist (siehe unter I 3.2).

1.2 Videoüberwachung öffentlich zugänglicher Räume

Die anstehende Regelung zur Videoüberwachung öffentlicher Räume und besonders gefährdeter Bereiche nicht öffentlich zugänglicher Bereiche von Dienstgebäuden im HmbDSG wird die Möglichkeit zur Videoüberwachung durch öffentliche Stellen zu Zwecken des Hausrechts und der Zugangskontrolle ermöglichen. Zugunsten der Betroffenen wird auf eine restriktive Handhabung zu achten sein.

Die durch öffentliche Stellen vorgenommene Videoüberwachung wurde von uns in der Vergangenheit mangels einer konkreten Regelung nach den allgemeinen Datenverarbeitungsvorschriften des Hamburgischen Datenschutzgesetzes (HmbDSG) und in analoger Anwendung der Maßstäbe der bundesgesetzlichen Regelung in §6b BDSG (Bundesdatenschutzgesetz) beurteilt (vgl. z.B. 20.TB, 12.2, 12.3).

Bereits am 23. Februar 2007 hatte das Bundesverfassungsgericht zu einer entsprechenden Rechtslage in Bayern festgestellt, dass die Videoüberwachung aufgrund der vielfältigen Auswertungsmöglichkeiten des gewonnenen Bildmaterials grundsätzlich einen derart schwerwiegenden Eingriff in das informationelle Selbstbestimmungsrecht der überwiegend rechtstreuen Betroffenen darstellt, dass dieser nur auf einer spezialgesetzlichen Grundlage erfolgen darf (vgl. näher 20.TB, 13.4).

Damit stand fest, dass auch in Hamburg die Videoüberwachung durch öffentliche Stellen einer ausdrücklichen Regelung bedarf. Für Sachverhalte, wie sie in jeder Dienststelle vorkommen, bot sich eine Regelung im HmbDSG als Querschnittsgesetz an, für spezifische fachliche Belange müssen Regelungen in Fachgesetze aufgenommen werden, wie dies bisher in den Bereichen Polizei (§8 des Gesetzes zur Datenverarbeitung der Polizei), Justiz (vgl. 6.1) und Schule (vgl. 4.1) geschehen ist.

Bereits Ende 2007 und Anfang 2008 hatte es erste Überlegungen für eine Regelung im HmbDSG gegeben, die jedoch in der 18. Legislaturperiode nicht mehr weiterverfolgt werden konnten. Dementsprechend hatte der Hamburgische Datenschutzbeauftragte im März 2008 im Rahmen der Koalitionsverhandlungen den Beteiligten zur Verbesserung des Datenschutzes eine Ergänzung des HmbDSG um eine klare, restriktive Regelung für die Videoüberwachung von öffentlichen Dienstgebäuden einschließlich Schulen empfohlen.

Im Sommer 2009 wurde das Thema durch zwei Kleine Anfragen der Linken (Drucksachen 19/3945 und 19/4127) in das öffentliche Interesse gerückt. Aus Anlass der Antwort des Senats, aus der sich eine hohe Dichte von behördlich betriebenen Videokameras ergab, haben wir die Forderung erhoben, die Kameraüberwachung auf eine rechtliche Grundlage zu stellen. Eine solche Regelung sollte aus unserer Sicht folgende Aspekte beinhalten:

Die Regelung sollte lediglich die allgemeinen Bedürfnisse aus Hausrecht und Zugangskontrollen umfassen; sonstige fachliche Bedarfe müssen in den einschlägigen Fachgesetzen spezifisch und restriktiv geregelt werden.

Im Hinblick auf die besondere Eingriffstiefe sollte es eine deutliche Abstufung in den Anforderungen an bloße Beobachtung und an Aufzeichnungen geben. Aufzeichnungen dürfen nur bei sich konkretisierender Gefahrenlage entsprechend

den Anforderungen im Polizeirecht erfolgen. Die weitere Nutzung für andere Zwecke sollte auf für die Rechtsordnung wesentliche Bereiche beschränkt sein.

Neben den allgemeinen Anforderungen an die Transparenz (Kennzeichnung der Überwachung und Benachrichtigung bei Zuordnung der Bilder zu einer Person) sollten die Einrichtung der Videoüberwachungsanlagen genauso wie andere Daten verarbeitende Anlagen vor Einführung einer Risikoanalyse unterzogen werden und in einer für Betroffene nachvollziehbaren Verfahrensbeschreibung dargestellt werden. Dies gewährleistet auch die notwendigen technisch-organisatorischen Maßnahmen zur Begrenzung der Aufnahmen auf das erforderliche Maß im Einzelfall, wie z.B. Einstellungen und Aufnahmezeiten.

Darüber hinaus wäre eine klarstellende Regelung für sinnvoll zu erachten, nach der akustische Überwachungen und die Anwendung von Attrappen verboten sind.

Wir werden uns dafür einsetzen, dass die künftige Regelung im Sinne des informationellen Selbstbestimmungsrechts der Betroffenen ausgestaltet wird. Dies gilt auch für bereits vorhandene Videoanlagen, für die der alte Rechtszustand keinen Bestandsschutz geschaffen hat.

2. Personaldaten

2.1 ePers/KoPers

Durch unsere frühzeitige Beteiligung und das Einbeziehen der datenschutzrechtlichen Anforderungen können bei der Neuausrichtung der IT-Unterstützung von Personalmanagementaufgaben nachträgliche und möglicherweise aufwändige Korrekturen vermieden werden.

Mit dem Projekt E-Personal beabsichtigt die Freie und Hansestadt Hamburg die Qualität der hamburgischen Personalprozesse nachhaltig zu stärken und deren Wirtschaftlichkeit zu sichern. Das Projekt umfasst u.a. die Ablösung der IT-Unterstützung von Personalverwaltungsaufgaben, die Einführung durchgängiger elektronischer Geschäftsprozesse, die Unterstützung neuer personalwirtschaftlicher Funktionalitäten und die Realisierung eines interaktiven Personalportals, in das alle personalwirtschaftlichen Fachverfahren integriert werden sollen. Wegen der parallelen Modernisierung der Haushaltsverfahren (s. Kap. III 3) besteht zusätzlich die Chance, die Einbindung der IT-Unterstützung von Personalmanagementaufgaben in ein Gesamtkonzept mit den Ressourcen steuernden Verfahren zu erörtern und zu entscheiden.

Es ist vorgesehen, das Projekt in Kooperation mit Schleswig-Holstein durchzuführen. Das Projekt strebt auf der Basis einer gemeinsamen IT-Organisation für personalwirtschaftliche Lösungen die gemeinsame Beschaffung und den gemeinsamen Betrieb der entwickelten Lösungen an. Der Kooperationsvertrag regelt vorlaufend Aufgaben, Ziele und Erfolgsfaktoren, Organisation sowie Kosten-Nutzen-Aspekte der Zusammenarbeit.

Drei Themenfelder bilden wesentliche Schwerpunkte:

- Entwicklung einer gemeinsamen personalwirtschaftlichen IT-Organisation mit SH;
- Auswahl, Anpassung und Einführung personalwirtschaftlicher IT-Systeme;
- Organisation und Optimierung der personalwirtschaftlichen Geschäftsprozesse der FHH.

Es ist erfreulich, dass wir bei diesem Entwicklungsprozess von Anfang an als Mitglied in den Lenkungsgruppen sowie in den einzelnen Arbeitsgruppen beteiligt sind.

2.2 Abwesenheits-/Krankenlisten

Für die Personaleinsatzplanung können Abwesenheitslisten nur ohne Angabe von Gründen außerhalb der Personalabteilung geführt werden.

Im Berichtszeitraum beschwerten sich immer wieder Beschäftigte, dass in den Fachabteilungen Abwesenheitslisten mit Angaben von Gründen, insbesondere über krankheitsbedingtes Fehlen, geführt werden. Diese Einsatzpläne oder Übersichten sind teilweise in Papierform oder elektronisch offen für alle Mitarbeiter zugänglich.

Personenbezogene Daten von Beschäftigten dürfen verarbeitet werden, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Beschäftigungsverhältnisses oder zur Durchführung organisatorischer, personeller oder sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung oder des Personaleinsatzes, erforderlich ist (§§ 28 Abs. 2 HmbDSG, 96 HmbBG a.F.). Durch technische und organisatorische Maßnahmen ist sicherzustellen, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können (§ 8 Abs. 2 Nr. 1 HmbDSG). Übersichten über Erkrankungen, Krankenstandsmitteilungen u.ä. sind Personalaktendaten, die nur dem in § 96a Abs. 3 HmbBG a.F. genannten Personenkreis zugänglich sein dürfen.

Fachvorgesetzte, die nicht zu diesem zugangsberechtigten Personenkreis gehören, können zum Zwecke der Personaleinsatzplanung eine Übersicht der abwesenden Beschäftigten, allerdings ohne Nennung von Gründen, führen. Auf welche Art und Weise, manuell, als Word-Tabelle, Excel-Tabelle, Access-Datenbank oder als gesonderter Outlook-Ordner, spielt dabei keine Rolle. Es kommt nicht darauf an, ob etwas nützlich ist oder der Arbeitserleichterung dient. Ausschlaggebend für eine zulässige Verarbeitung von personenbezogenen Daten ist das Vorliegen einer Rechtsgrundlage.

Der für die Personaleinsatzplanung Verantwortliche gehört mit seinem Vertreter zu den zugangsberechtigten Personen. Wird die Übersicht so geführt, dass nur erkennbar ist, wer abwesend ist – ohne Angabe des Grundes -, kann die Kenntnisnahme durch andere Kollegen in der Abteilung hilfreich sein.

2.3 Angaben über Arbeitsunfähigkeitszeiten im Bewerbungsverfahren

Der Arbeitgeber kann eine Bescheinigung der Krankenkasse über Arbeitsunfähigkeitszeiten nicht vom Bewerber verlangen.

Wir wurden auf eine besondere Stellenausschreibung aufmerksam gemacht. Auszug:

„Neben einem tabellarischen Lebenslauf und Angaben zum beruflichen Werdegang wird eine Bescheinigung der Krankenkasse über die Zeiten der Arbeitsunfähigkeit der letzten 3 Jahre verlangt."

Eine Rechtsgrundlage zur Erhebung solcher Daten lag nicht vor. Nach unserem Hinweis wurden Bescheinigungen der Krankenkasse über Arbeitsunfähigkeitszeiten nicht mehr gefordert. Nicht nur wir, sondern auch das Personalamt als Oberste

Dienstbehörde in Personalangelegenheiten ist tätig geworden und hat diese Art der Datenerhebung untersagt.

3. Finanzen und Steuern

Haushaltsverfahren: Anforderungen werden nicht erfüllt

Die Dokumentation des Verfahrens SAP für Hamburg wird nicht zeitnah fortgeschrieben. Wieder wurden Originaldaten, die für Testzwecke genutzt worden waren, nicht unverzüglich gelöscht.

Für die Prozesse in der Kasse, der Mittelbewirtschaftung und der Anlagenbuchhaltung nutzt die FHH ein komplexes SAP-System. Die Fachliche Leitstelle, die zur Finanzbehörde/Amt für Haushalt und Aufgabenplanung gehört, ist verantwortlich für die Vorgaben für die Programmierung und die Systemaussteuerung, testet und gibt auch die laufenden Änderungen frei.

Der HmbBfDI hat sich in den Jahren 2007 und 2008 wiederholt darum bemüht, eine aktuelle Dokumentation des Berechtigungskonzepts für das IT-Verfahren SAP für Hamburg zu erhalten. Auch eine Dokumentation des Tests mit Originaldaten zum Umstieg auf SAP ERP 6.0 zum 1. Januar 2009, deren Zusendung die Fachliche Leitstelle zugesagt hat, hat der HmbBfDI trotz Nachfrage nicht erhalten. Diese unzureichende Information des HmbBfDI war Anlass für die Prüfung des Verfahrens SAP mit dem Schwerpunkt Dokumentation des Verfahrens.

Die Anforderungen an die Dokumentation eines produktiven IT-Verfahrens sind in der Freigaberichtlinie differenziert festgeschrieben. Danach ist die Fachliche Leitstelle dafür verantwortlich, dass die Dokumentation jederzeit vollständig und inhaltlich auf dem aktuellen Stand zur Verfügung steht. Verfahrens- und Softwareänderungen müssen in der Dokumentation zeitlich und inhaltlich nachvollzogen werden können. Die Dokumentation besteht aus der

- Verfahrensdokumentation und -beschreibung,
- Dokumentation für die Rechenstelle,
- Benutzerdokumentation und der
- Softwaredokumentation.

Der Rechnungshof hat bereits im Rechnungshofbericht vom 7. Februar 2007 auf eine nicht vollständige Dokumentation des Verfahrens hingewiesen und die Finanzbehörde aufgefordert, die Dokumentationsanforderungen unverzüglich umzusetzen. Die Finanzbehörde hatte damals bestätigt, dass die Verfahrensdokumentation zu verbessern ist. Bei der Prüfung durch den HmbBfDI im März 2009 hat die Fachliche Leitelle jedoch erneut erklärt, dass aus ihrer Sicht bei der Dokumentation noch wesentliche Verbesserungsnotwendigkeiten erforderlich sind und auch der derzeitige Stand nicht den Anforderungen entspricht. Damit hat die Fachliche Leitstelle die ihr übertragenen Aufgaben nicht im erforderlichen Umfange wahrgenommen.

Als Reaktion auf den Rechnungshofbericht wurde ein Projekt Dokumentation in der Fachlichen Leitstelle SAP aufgelegt. Dazu gibt es jedoch keine Projektbeschreibung und eine Projektplanung ist nicht vorhanden. Die Fachliche Leitstelle SAP hat den Beschluss gefasst, die Dokumentation nicht mehr in Form von ergänzenden Word-Dokumenten vorzunehmen. Diese Form hat sich als nicht praktikabel heraus-

gestellt, weil innerhalb kurzer Zeit die Dokumentation und der Ist-Stand auseinandergelaufen sind. Die entsprechenden Dokumente wurden nicht nachgepflegt.

Die neue Dokumentationsform erfolgt im SolutionManager, den SAP zur Verfügung stellt. Es wurde auch festgelegt, dass eine vollständige Dokumentation aufgrund der bereits festgelegten Ablösung des Verfahrens bis 2013 nicht erfolgen soll, aber wichtige Bereiche zu dokumentieren sind. Die neue Form der Dokumentation wurde in einem ersten Bereich umgesetzt. Dadurch haben alle Entwickler und die Fachliche Leitstelle die Möglichkeit, sofort Änderungen zu dokumentieren und es müssen keine getrennten Dokumente in einem separaten Textverarbeitungsprogramm verfasst bzw. gepflegt werden. Auch lassen sich mit diesem System Aufträge etwa zum Testen von Programmänderungen anstoßen und verwalten, so dass diese unmittelbar in die Dokumentation einfließen können. Die Fachliche Leitstelle geht nach ihren ersten Erfahrungen davon aus, dass mit diesem System eine auf Dauer aktuell gehaltene Dokumentation erreicht werden kann.

Das Berechtigungssystem ist bisher nicht vollständig nach dem neuen Dokumentationsstandard dokumentiert. Wann dieses erfolgt sein wird, konnte nicht benannt werden. Vor dem Hintergrund des sehr komplexen Berechtigungssystems in SAP und der Tatsache, dass die Vertraulichkeit des hamburgweiten Systems wesentlich auf diesem basiert, ist dies äußert kritisch. Vor dem Hintergrund, dass das derzeitige System noch mindestens drei Jahre genutzt wird, sollte gerade die Dokumentation des Berechtigungssystems auf einem aktuellen Stand gehalten werden. Um auch dessen anforderungsgerechte Umsetzung zu kontrollieren, sollte darüber hinaus eine toolgestützte Überprüfung durchgeführt werden.

Auch die überprüfte Dokumentation des Tests mit Originaldaten ergab Mängel. Positiv ist hervorzuheben, dass es einen differenzierten Testplan gab. Es wurden jedoch zahlreiche Testkonstellationen aufgeführt, die als „nicht erledigt" gekennzeichnet waren. Die Nutzung von Originaldaten für Testzwecke ist nur zulässig, wenn die Voraussetzungen der Freigaberichtlinie erfüllt werden. Ob diese vollständig gegeben waren, ließ sich im Einzelnen nicht nachvollziehen, wie eine Dokumentation z.B. des Aufwandes für Anonymisierung der Daten und der an den Tests beteiligten Personen nicht vorlag. Insbesondere ist jedoch zu kritisieren, dass die Originaldaten auch viereinhalb Monate nach dem Produktivstart immer noch nicht gelöscht waren. Vor dem Hintergrund, dass der HmbBfDI bereits im 21.TB, 2.3 einen gravierenden Mangel beim Test mit Originaldaten beim SAP-Verfahren dokumentiert und auch gerade die zeitnahe Löschung der Produktivdaten nach dem Abschluss solcher Tests eindringlich eingefordert hat, ist dies besonders bedenklich und zeigt, dass hier nach wie vor Handlungsbedarf seitens der Finanzbehörde besteht.

4. Polizei

4.1 Novellierung des Polizeirechts

Erforderliche Änderungen wurden im Gesetz über die Datenverarbeitung der Polizei (PolDVG) noch immer nicht umgesetzt. Für den Fall, dass Online-Durchsuchungen in den Katalog der verdeckten Ermittlungsmaßnahmen des PolDVG aufgenommen werden, sind die Vorgaben des Bundesverfassungsgerichts zu beachten.

Bereits im vorletzten Tätigkeitsbericht (20. TB, 7.2) hatten wir darauf hingewiesen, dass die Regelungen zur präventiven Telekommunikationsüberwachung in § 10a PolDVG an die Rechtsprechung des Bundesverfassungsgerichts vom 27. Juli 2005

(1 BvR 668/04) zum niedersächsischen Polizeirecht angepasst werden müssen (siehe auch III 4.2). Dabei sollte zumindest der Standard des § 100a der inzwischen novellierten Strafprozessordnung (StPO) zum Schutz des Kernbereichs privater Lebensgestaltung erreicht werden.

Im letzten Tätigkeitsbericht (21. TB, 8.1) hatten wir dargelegt, dass auch die Regelungen der optischen und akustischen Wohnraumüberwachung nach § 10 Abs. 2 PolDVG an die Anforderungen des Kernbereichsschutzes anzupassen sind.

Ebenfalls im 21. Tätigkeitsbericht (8.1) hatten wir auf zwischenzeitlich weitere Änderungsbedarfe für die Rasterfahndung nach § 23 PolDVG hingewiesen. Diese ergeben sich aus dem Beschluss des Bundesverfassungsgerichts vom 4. April 2006 (1 BvR 518/02). Die Rasterfahndung muss an das Vorliegen einer konkreten Gefahr geknüpft werden.

Inzwischen hat das Bundesverfassungsgericht in einer Entscheidung vom 27. Februar 2008 (1 BvR 370/07) zwar präventive Online-Durchsuchungen nicht grundsätzlich ausgeschlossen, aber deutliche Grenzen gezogen. Durch die tief greifende Veränderung der neuen Telekommunikationsmittel entwickeln sich neue, tief greifende Gefahren für das Persönlichkeitsrecht der Bürgerinnen und Bürger. Deshalb hat das Bundesverfassungsgericht dargelegt, dass sich aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes (GG) auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ergibt. Soweit die Telekommunikationsinhalte vom staatlichen Eingriff berührt sind, ist Artikel 10 GG (Fernmeldegeheimnis) zu beachten. Soweit eine Infiltration – z. B. durch Trojaner – durch technische Manipulation am Rechner des Betroffenen in seiner Wohnung vorgenommen wird, gilt Artikel 13 GG (Unverletzlichkeit der Wohnung). Der Einsatz von Trojanern ist nach dem Urteil nur möglich bei existenzieller Gefährdung des Lebens, des Bestands des Staates oder der Versorgungseinrichtungen, die für die menschliche Existenz erforderlich sind. Auch die Grenzen, die das Gericht für den Kernbereichsschutz ausgeführt hat, haben Auswirkungen auf den Spielraum des Hamburgischen Gesetzgebers, bei einer Novellierung des Gesetzes über die Datenverarbeitung der Polizei eine Online-Durchsuchung zu regeln.

Mit Urteil vom 11. März 2008 (1 BvR 207/05) hat das Bundesverfassungsgericht die Regelungen über die automatisierte Kraftfahrzeug-Kennzeichenerfassung nach dem Schleswig-Holsteinischen Landesverwaltungsgesetz und dem Hessischen Sicherheits- und Ordnungsgesetz für nichtig erklärt (siehe unten III 4.3).

Soweit Sprachaufzeichnungen der Notrufe und sonstigen in der PEZ ein- und ausgehenden Telefonate zu Gefahrenabwehrzwecken erfolgen, bedarf es einer gesetzlichen Regelung. Die Speicherung der Sprachaufzeichnung erfolgt derzeit für 60 Tage und dient unter anderem der Einsatzdokumentation, der Sicherstellung als Beweismittel im Rahmen der Strafverfolgung und dem Schutz der Beamten vor ungerechtfertigten Anschuldigungen. Auf unsere Nachfrage, zuletzt im Juli 2008, wurde uns von der Behörde für Inneres mitgeteilt, dass im Rahmen der Novellierung des PolDVG und des SOG (Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung) auch die Aufzeichnung von Notrufen und sonstigen in der Polizeieinsatzzentrale eingehenden Notrufe auf eine sichere Rechtsgrundlage gestellt werden sollen.

Der Hamburger Senat hatte zunächst bereits für das Jahr 2006 einen Referentenentwurf eines überarbeiteten PolDVG angekündigt (vgl. 21. TB, 8.1). In seiner Stel-

lungnahme zum 21. Tätigkeitsbericht hatte der Senat angegeben, das Urteil des Bundesverfassungsgerichts zur Online-Durchsuchung abwarten zu wollen (Drucksache 19/1383, Seite 4). Mitte 2008 war aus der Behörde für Inneres zu erfahren, ein Gesetzentwurf werde nach der Sommerpause vorliegen. Ein Entwurf lag jedoch bis Redaktionsschluss nicht vor. Über die aktuell beabsichtigten Änderungen der federführenden Behörde für Inneres konnten wir nichts erfahren.

4.2 Präventive Telekommunikationsüberwachung

Durch die „Unterrichtung der Bürgerschaft gemäß Artikel 5 des Gesetzes zur Erhöhung der öffentlichen Sicherheit in Hamburg" (Drucksache 19/2732 vom 7. April 2009) haben wir erfahren, dass es vom 29. Juni 2005 bis 30. Juni 2008 in 7 Sachverhalten zu 14 präventiven Telefonüberwachungen nach § 10a des Gesetzes über den Datenschutz der Polizei (PolDVG) gekommen war.

Im vorangegangenen Tätigkeitsbericht (21. TB, 8.1) hatten wir an den Anpassungsbedarf des § 10a PolDVG – insbesondere Abs. 1 – in Verbindung mit § 10c PolDVG erinnert (siehe auch oben III 4.1). Wir halten für die Telekommunikationsüberwachung weiter gehende Schutzbestimmungen für den Kernbereich der persönlichen Lebensgestaltung für erforderlich. Es ist ferner zu überdenken, ob die in § 10a Abs. 1 Satz 1 PolDVG aufgezählten Rechtsgüter allesamt einen schweren Eingriff in das Telekommunikationsgeheimnis rechtfertigen können. Eine unmittelbare Gefahr für den Leib einer Person besteht bereits dann, wenn eine (auch nur geringfügige) Körperverletzung droht. Dies scheint angesichts des schwer wiegenden Eingriffs in das Telekommunikationsgeheimnis nicht angemessen. Zumindest müssten Eingriffe nach § 10a Abs. 1 PolDVG auf Straftaten von erheblicher Bedeutung (§ 1 Abs. 4 PolDVG) beschränkt werden. Vorzugswürdig wäre allerdings eine weitere Einengung, mindestens auf das Maß der schweren Straftaten des § 100a Abs. 2 Strafprozessordnung (StPO), mit der zusätzlichen Einschränkung, dass die Tat auch im Einzelfall schwer wiegen muss (vgl. § 100a Abs. 1 Nr. 2 StPO).

Der gerade novellierte § 100a StPO zur repressiven Telekommunikationsüberwachung ist bereits wieder Gegenstand einer Beschwerde vor dem Bundesverfassungsgericht (1 BvR 601/08). Zwar hat das Bundesverfassungsgericht in seinem Beschluss vom 15. Oktober 2008 den Antrag auf Erlass einer einstweiligen Anordnung gegen die Anwendung des § 100a StPO abgelehnt (2 BvR 236/08). Allerdings hat es festgestellt, dass die Verfassungsbeschwerde weder von vornherein unzulässig noch offensichtlich unbegründet sei. Eine Aussetzung des Vollzugs der angegriffenen Normen bis zur Entscheidung im Hauptsacheverfahren könne nur deshalb nicht ergehen, weil sich das Überwiegen der dafür sprechenden Gründe nicht feststellen lasse. Um den Vollzug des Gesetzes außer Kraft zu setzen, hätten die für eine vorläufige Regelung sprechenden Gründe so schwer wiegen müssen, dass sie den Erlass einer einstweiligen Anordnung unabdingbar machen.

Uns wurde Ende 2008 gemäß § 26 PolDVG die Errichtungsanordnung für eine Datei zur Speicherung von Daten aus einer Telefonüberwachung nach § 10a Abs. 1 PolDVG vorgelegt. Aus dem Zusammenhang konnten wir entnehmen, dass die Telefonüberwachung erfolgte, um das Leben einer Person zu schützen, die von einem „Ehrenmord" bedroht war. In einem solchen Fall scheint eine präventive Telefonüberwachung durchaus erforderlich. Allerdings mussten wir trotzdem darauf hinweisen, dass die Rechtsgrundlage, auf die die Telefonüberwachung gestützt wurde, nicht den Vorgaben des Bundesverfassungsgerichts für die präventive Telefonüberwachung entsprach. Wir haben gefordert, falls die Datei in diesem beson-

deren Einzelfall dennoch weiter geführt würde, zumindest in der Errichtungsanordnung festzulegen, dass ein verfassungsgemäßer Kernbereichsschutz gewährleistet wird, und aus dem Kreis der Betroffenen, über die personenbezogene Daten gespeichert werden dürfen, „Dritte" zu streichen. Dieser Überlegung ist die Polizei gefolgt.

Neben einer weiteren Telefonüberwachungsdatei, die Mitte Dezember 2005 errichtet und uns erst Anfang 2006 (nach Ende der Maßnahme) vorgelegt worden war, waren uns keine weiteren präventiven Telekommunikationsüberwachungen bekannt geworden. Erst aus der Unterrichtung der Bürgerschaft gemäß Artikel 5 des Gesetzes zur Erhöhung der öffentlichen Sicherheit in Hamburg haben wir erfahren, dass es im Zeitraum Dezember 2005 bis März 2008 insgesamt 7 Telefonüberwachungen mit 14 überwachten Anschlüssen gegeben hat. In 4 von 7 Fällen erfolgte die Anordnung zur Telefonüberwachung durch den Polizeipräsidenten bzw. seinen Vertreter. In einem dieser Fälle wurde die richterliche Bestätigung nachgeholt. Unsere Nachfrage ergab, dass nur in 2 Fällen Gesprächsinhalte aufgezeichnet wurden; nur in einem Fall wurde hierfür eine Datei errichtet, die uns vorgelegt worden war. In 5 der 7 Fälle sei die Abwehr der Gefahr für Leib oder Leben nur möglich gewesen, weil sich aus den Telefonüberwachungen maßgebliche Erkenntnisse ergeben hätten. – Diese Zahl der präventiven Telefonüberwachungen lässt eine Änderung der §§ 10a und 10c PolDVG nach den Maßstäben des Bundesverfassungsgerichts umso dringlicher erscheinen. Außerdem lösen diese Beispiele aus der Praxis die Überlegung aus, Telefonüberwachungen stets von einem Richter überprüfen zu lassen, auch wenn sie vom Polizeipräsidenten angeordnet wurden und die Maßnahmen bereits vor Ablauf von 3 Tagen beendet wurden.

4.3 Kraftfahrzeug-Kennzeichenerfassung

Die Polizei Hamburg wendet seit dem Urteil des Bundesverfassungsgerichts zum Kennzeichenscanning nach hessischem und schleswig-holsteinischem Recht § 8 Abs. 6 des Gesetzes über den Datenschutz der Polizei (PolDVG) nicht mehr an. Ob bei einer Novellierung des PolDVG eine neue Rechtsgrundlage für die Kennzeichenerfassung geschaffen werden soll, ist uns nicht bekannt.

Wir hatten uns mit den in Hamburg eingesetzten „automatischen Kennzeichenlesesystemen" (AKLS) befasst, die im Jahr 2007 mehrfach im Blickwinkel der Öffentlichkeit standen. Mit ihnen hatte die Polizei seit Mai 2006 bis zur Entscheidung des Bundesverfassungsgerichts vom 11. März 2008 (1 BvR 2074/05) im fließenden Verkehr Kennzeichen vorbeifahrender Fahrzeuge elektronisch erfasst, um sie mit Sachfahndungsbeständen der Datei INPOL und des Schengener Informationssystems (S.I.S.) abzugleichen.

Die Hamburgische Regelung des Kennzeichenscannings in § 8 Abs. 6 SOG ist nahezu wortgleich mit der nichtigen Regelung im Schleswig-Holsteinischen Landesverwaltungsgesetz, so dass sich die vom Bundesverfassungsgericht am 11. März 2008 herausgestellten Mängel auf § 8 Abs. 6 PolDVG übertragen lassen. Wenn ein Abgleich der Kennzeichen mit dem Fahndungsbestand nicht unverzüglich erfolge und das Kennzeichen nicht ohne jede weitere Auswertung sofort und spurenlos gelöscht werde, greife die Maßnahme in den Schutzbereich des Grundrechts auf informationelle Selbstbestimmung ein, so das Bundesverfassungsgericht. Den beanstandeten Normen fehle es an näheren Voraussetzungen für die Maßnahme, insbesondere an einer hinreichenden bereichsspezifischen und normenklaren Bestimmung des Anlasses und des Verwendungszwecks der automatisierten Erhe-

bung. Der eigentliche Ermittlungszweck bleibe ebenso offen wie der Begriff des „Fahndungsbestands". Damit sei auch der Verwendungszweck der erhobenen Daten unklar. Die automatisierte Erfassung der Kennzeichen dürfe nicht anlasslos erfolgen oder flächendeckend durchgeführt werden. Ohne Anknüpfung an konkrete Gefahrenlagen, gesteigerte Risiken von Rechtsgutsgefährdungen oder Rechtsgutsverletzungen fehle die Verhältnismäßigkeit im engeren Sinne.

Die Polizei Hamburg führt im Hinblick auf die verfassungsgerichtliche Entscheidung derzeit keine Kennzeichenerfassung durch. Bei einer Neuregelung hätte der Landesgesetzgeber auch zu beachten, dass die bisherige gesetzliche Regelung die Erhebung und weitere Verarbeitung von Bildmaterial vom Fahrzeuginneren nebst Insassen, welches bisher angefallen war, nicht umfasst. Ob § 8 Abs. 6 PolDVG im Zuge der anstehenden Novellierung ersatzlos gestrichen oder an die Vorgaben des Bundesverfassungsgerichts angepasst wird, ist abzuwarten. Jedenfalls wird der Landesgesetzgeber die Grenzen der Gesetzgebungskompetenz zu beachten haben, die es ausschließen dürften, die Kennzeichenerfassung zu Zwecken zu regeln, die im Schwerpunkt einer Strafverfolgung dienen.

Der Senat hatte im Rahmen einer Kleinen Anfrage im Juli 2007 ausführlich über den Einsatz der AKLS berichtet (Drucksache 18/6618). Schon aufgrund des Umstands, dass die AKLS nach den Senatsangaben sehr viele fehlerhafte Treffermeldungen anzeigen, haben wir Vorbehalte gegen eine neue Rechtsgrundlage für das Kennzeichenscanning. Bestenfalls wurde im praktischen Einsatz eine fehlerhafte Meldung erkannt, bevor betroffene Autofahrer und weitere Fahrzeuginsassen unnötig angehalten und ihre Personalien überprüft wurden. Bei Fehlern, die nicht auf technischen Lesefehlern des AKLS beruhen, sondern auf nicht aktualisierten Inhalten der INPOL- und S.I.S.-Dateien, wurden Autofahrer stets angehalten und überprüft. Nach den Erfahrungen der ersten 14 Monate des AKLS-Einsatzes führten nur 0,22 % der gescannten Kennzeichen zu Treffermeldungen. 71,1% dieser (0,22 %) Treffermeldungen waren fehlerhaft (vgl. Drucksache 18/6618, Seite 2 f.). Während Aufnahmen mit Nichttreffer-Kennzeichen laufend überschrieben werden, wurden fehlerhafte Treffermeldungen erst nach Einsatzende manuell gelöscht.

4.4 Videoüberwachung Reeperbahn und Hansaplatz

Die unkomfortable Videotechnik soll verbessert werden. Bisherige Ergebnisse sprechen nicht für die Eignung der Videoüberwachung zur Gefahrenabwehr.

Im vorangegangenen Tätigkeitsbericht (21. TB, 8.2) hatten wir über unsere Prüfung berichtet. Wir hatten beschrieben, dass der Schutz der „private zones", also der privaten Bereiche, vor allem der Wohnungen, dadurch gewahrt wird, dass der gesamte Bildschirm durch Verpixelung schwarz wird und eine Aufzeichnung unterbleibt, sobald bei der Bewegung der Kamera eine „private zone" am Rande gestreift wird. Dann ist es für die am Kamerabedienplatz eingesetzten Beamten sehr schwierig, mit dem Joystick den zuletzt betrachteten Bildausschnitt überhaupt wieder anzusteuern. Dies schränkt die Eignung der Videoüberwachung zur Gefahrenabwehr besonders dann ein, wenn ein Geschehnis bzw. eine Person mit der Kamera verfolgt werden soll. Inzwischen hat die Lieferfirma den Auftrag erhalten, eine neue Verpixelungstechnik zu entwickeln. Die neue Technik wurde uns erläutert und demonstriert. Die „private zones" sollen zukünftig vorab so markiert werden, dass nur die markierten Bereiche geschwärzt werden, während die umgebenden Bereiche auf dem Überwachungsmonitor sichtbar bleiben. Das erleichtert den Betrach-

tern die Orientierung und die Beobachtung. Im Juni 2009 hat die Polizei die voraussichtliche Entwicklungsdauer der neuen Software mit ca. 10 Monaten angegeben.

Im vorangegangenen Tätigkeitsbericht hatten wir unsere Forderung, noch vor der Inbetriebnahme der Videoüberwachung des Hansaplatzes eine unabhängige Evaluierung der Videoüberwachung der Reeperbahn vorzulegen, unterstrichen. Dies war von der Polizei abgelehnt worden. Der Senat hat gegenüber der Bürgerschaft angekündigt, jeweils nach Ablauf der dreijährigen Betriebszeit der Videoüberwachung der Reeperbahn und des Hansaplatzes nach dem 30. März 2009 bzw. 3. Juli 2010 gesonderte Wirksamkeitsanalysen vorzulegen (vgl. Drucksache 19/2732, Seite 6). Leider ergab unsere Nachfrage bei der Polizei im September 2009, dass die Wirksamkeitsanalyse zur Videoüberwachung Reeperbahn behördenintern erstellt wird. Unserer Vorstellung von einer unabhängigen Evaluierung entspricht dies nicht. Zudem ist derzeit offen, ob und wie ihre Ergebnisse, die noch innerhalb der Behörde für Inneres abgestimmt werden, veröffentlicht werden. Wir werden den abgestimmten Bericht, der im ersten Quartal 2010 vorliegen soll (Drucksache 19/4282, Seite 3), anfordern und kritisch beleuchten. Insbesondere werden wir ein Augenmerk darauf haben, ob die Wirksamkeitsanalyse die Schlussfolgerung zulässt, dass die Videoüberwachung selbst und nicht die zeitgleich erhöhte Polizeipräsenz (vgl. Drucksache 19/2732, Seite 6) etwaige Verbesserungen für die öffentliche Sicherheit erbracht hat. Außerdem erhoffen wir Aufschluss darüber, ob die Aufzeichnung der Kamerabilder für Gefahrenabwehrzwecke überhaupt notwendig ist; möglicherweise lassen sich Gefahrenabwehrzwecke auch durch bloße Beobachtung erreichen.

Nach den Angaben des Senats über die Ergebnisse der Videoüberwachung der Reeperbahn in der „Unterrichtung der Bürgerschaft gemäß Artikel 5 des Gesetzes zur Erhöhung der öffentlichen Sicherheit in Hamburg" (Drucksache 19/2732 vom 7. April 2009) kommen wir allerdings bisher zu der vorläufigen Auffassung, dass die derzeitige Videoüberwachung der Reeperbahn keine präventive Wirkung entfaltet. Es zeigt sich, dass vor allem die registrierten Fallzahlen derjenigen Delikte, die ohnehin zahlenmäßig am häufigsten auftreten (einfache / fahrlässige Körperverletzung, gefährliche / schwere Körperverletzung), in dem 3-Jahres-Zeitraum stark gestiegen ist. Die registrierten Fallzahlen der einfachen / fahrlässigen Körperverletzungen sind: Im 1. Jahr 369, im 2. Jahr 498, im 3. Jahr 526. Die Angaben für gefährliche / schwere Körperverletzung betragen: Im 1. Jahr 182, im 2. Jahr 222, im 3. Jahr 235. Zwar hat die Polizei festgestellt, dass in angrenzenden Kontrollbezirken die registrierten Fallzahlen ebenfalls gestiegen seien, aber dennoch bleiben die Schlussfolgerungen, die die Polizei daraus zu ziehen versucht, spekulativ. Theoretisch sind für den Anstieg der registrierten Delikte mehrere Ursachen denkbar. Die Anzahl der tatsächlich verübten Delikte könnte gestiegen sein. Wenn dieser Umstand zuträfe, könnte eine positive gefahrenabwehrende Funktion der Videoüberwachung daraus nicht gefolgert werden. Eine weitere Möglichkeit ist, dass durch die Videoüberwachung mehr Delikte registriert werden (Dunkelfelderhellung). Auch dieser Umstand könnte aber nicht belegen, dass die Videoüberwachung eine gefahrenabwehrende Funktion besitzt. Eine weitere denkbare Variante der Dunkelfelderhellung wäre eine verstärkte Anzeigebereitschaft der Opfer oder Zeugen. Daraus könnte ebenso wenig die Schlussfolgerung erwachsen, Videoüberwachung sei zur Gefahrenabwehr geeignet. Auch die Aussage, einen Verdrängungseffekt gebe es nicht, weil die Fallzahlen in den Kontrollgebieten weniger stark gestiegen seien als im überwachten Bereich, muss notgedrungen Spekulation bleiben. Eine Differenzierung zwischen der Eignung der Videobeobachtung und der

Videoaufzeichnung zur Gefahrenabwehr erfolgt nicht. Es spricht nach dem gegenwärtigen Sachstand nichts dafür, dass die Aufzeichnung der Bilder und die dreißigtägige Speicherung dazu genützt hätten, eine Gefahr abzuwenden.

Aufgrund umfangreicher Baumaßnahmen zur Umgestaltung des Hansaplatzes wird die Videoüberwachungstechnik mindestens für den Zeitraum der Baumaßnahmen abgebaut; nach Angaben des Senats wäre ein Wiederaufbau nach Abschluss der Baumaßnahmen möglich (Drucksachen 18/2823 und 19/4282). Wir werden zu gegebener Zeit mit der Polizei erörtern, ob eine erneute Installation der Kameras im Sinne des § 8 Abs. 3 PolDVG zu Zwecken der Gefahrenabwehr geeignet, erforderlich und angemessen ist. Dabei wird auch differenziert zu bewerten sein, ob im Falle einer erneuten Installation die Beobachtung zeitlich begrenzt wird und eine Aufzeichnung unterbleibt.

4.5 Kontrolle der Zugriffsprotokollierungen

Die Effektivität der Zufallsprotokollierungen in den Dateien POLAS, ComVorIndex und EWO lässt sich bislang nicht messen und entspricht nicht den gesetzlichen Anforderungen an technisch-organisatorische Maßnahmen.

Mit den notwendigen Zugriffsmöglichkeiten der Bediensteten der Polizei Hamburg auf Datenbanken sind zwangsläufig Missbrauchsmöglichkeiten verbunden. Unerlaubte Zugriffe können aus privaten Motiven erfolgen, z. B., um aus eigenen Interessen oder im Interesse Dritter etwas über Nachbarn, Bekannte, Mietinteressenten oder über Prominente in Erfahrung zu bringen.

Natürlich wird jeder Zugriff auf die polizeilichen Datenbanken protokolliert. Bis zum Jahr 2005 waren Kontrollen der so erzeugten Protokolldateien nur nicht automatisiert erfolgt. Aufgrund des öffentlichen Interesses am polizeilichen Umgang mit Daten hatte die Innenrevision der Behörde für Inneres (BfI) im Jahr 2000 eine Prüfung durchgeführt und anschließend gefordert, ein geeignetes Verfahren zur Stichprobenkontrolle zu implementieren, um den Anforderungen des § 8 des Hamburgischen Datenschutzgesetzes (HmbDSG) gerecht zu werden.

2005 wurden wir von der Polizei über die Planungen informiert, zunächst in einer Pilotierung automatisierte Zufallsstichproben in POLAS einzuführen und nach einem Jahr zu evaluieren. Wir haben uns vor allem dafür eingesetzt, ein Dokumentationsverfahren vorzusehen, das die Ergebnisse der Stichprobenkontrollen auswertbar erfasst und qualitätssichernde Maßnahmen ermöglicht. Uns wurde damals mitgeteilt, dass unsere fachlich berechtigten Anregungen nur durch eine zusätzliche automatisierte Umsetzung realisiert werden könnten, wovon jedoch wegen des zeitnah geplanten Starttermins und aus Kostengründen zunächst abgesehen würde. Unsere Anregungen könnten nach der Evaluierung gegebenenfalls erst in einer 2. Version des computergestützten Stichprobenverfahrens berücksichtigt werden.

Die Polizei hat dann in den Dateien POLAS (Polizeiliches Auskunftssystem), ComVorIndex (computergestützte Vorgangsverwaltung) und EWO (Einwohnermeldewesen) im Zeitraum Juli 2006 bis Januar 2007 sukzessive Zufallsprotokollierungen eingeführt. Bei jedem 500. Zugriff auf die Datenbanken wird automatisch eine Kontrollmitteilung erzeugt. Die abfragenden Bediensteten erhalten dann bei einem Datenzugriff eine Abfragemaske auf dem Bildschirm. Die Kontrollmitteilungen werden an spezielle Datenschutzpostfächer gesendet, auf die die Dienstvorgesetzten bzw. von diesen ermächtigte nachgeordnete Vorgesetzte Zugriff haben. Die Dienstvor-

gesetzten sind im Rahmen ihrer Fachaufsicht gehalten, die Abfrageberechtigung zu überprüfen und bei unberechtigten Abfragen Maßnahmen zu ergreifen.

Nachdem wir keine weiteren Informationen oder einen Evaluationsbericht von der Polizei erhielten, fragten wir im Sommer 2008 nach, welche Ergebnisse die Zufallsprotokollierungen gebracht haben. Wir erhielten die Mitteilung, dass über das Stichprobenverfahren keine Dokumentation erfolge. Man vertraue darauf, dass die Dienststellenleiter die Kontrollen durchführen. Auch Verstöße und Konsequenzen bzw. Maßnahmen würden nicht systematisch erfasst. Eine Information der Leitungsebene der Polizei über die Ergebnisse der Stichprobenkontrollen erfolge nicht.

Da die Innenrevision der Bfl im ersten Halbjahr 2007 eine Überprüfung des Stichprobenverfahrens durchgeführt hatte, wollten wir zunächst deren Ergebnis abwarten, bevor wir Planungen zu einer eigenen Überprüfung ergreifen. Im September 2009 wurde uns endlich ermöglicht, wenigstens Einblick in den Prüfbericht zu nehmen, dessen Endfassung im Dezember 2008 innerhalb der Bfl abgestimmt worden war. Aus dem Bericht haben wir geschlossen, dass eine Überprüfung der durchgeführten Stichproben sehr schwierig und nur eingeschränkt möglich ist. Die Innenrevision hatte versucht, über 6.000 Zufallsprotokollierungen selbst auszuwerten, da sie auf keine Dokumentation von Seiten der Polizei zurückgreifen konnte. Da die Abfragemasken von den Bediensteten nur optional ausgefüllt werden müssen, waren die Abfragefelder „Anlass" und „im Auftrag" häufig nicht oder mit dem Eintrag „keine Angabe" oder der Abfragegrund mit ungebräuchlichen Abkürzungen ausgefüllt worden. Außerdem wurde nur in 44 % der Fälle ein Aktenzeichen angegeben.

Auf unsere Nachfrage ließ die Polizei Ende 2009 wissen, für eine Verfahrensänderung habe durch das Evaluationsergebnis 2007 aus Sicht der Polizei keine Veranlassung bestanden. Vom 1. August bis 31. Oktober 2009 sei ein zur Zufallsprotokollierung flankierendes Verfahren eingezogen worden. Überprüft worden sei das freiwillige Eintrageverhalten der Mitarbeiter und die Frage, ob die Vorgesetzten ihrer Kontrollpflicht nachgekommen seien. Über 96 % der Abfragemasken seien freiwillig ausgefüllt worden; eine missbräuchliche Datenabfrage sei nicht festgestellt worden. 100 % der Vorgesetzten seien ihrer Kontrollpflicht nachgekommen.

Diese zeitlich begrenzte Kontrolle der Zufallsprotokollierungen ist aus unserer Sicht nicht ausreichend. Die Polizei hat das genaue Vorgehen nicht beschrieben. Wenn in 96 % der Zufallsprotokollierungen die Beschäftigten Einträge in die Abfragemaske vorgenommen haben, lässt dies auf die Vollständigkeit und Nachvollziehbarkeit dieser Hinweise zum Grund der Abfrage keine Rückschlüsse zu. Andererseits: Wenn 96 % der Abfragenden freiwillig Angaben gemacht haben, spricht nichts dagegen, das Ausfüllen der Abfragemaske für die Bediensteten zur Pflicht zu machen – soweit nicht besondere Eile wegen Gefahr im Verzug geboten ist. Damit könnten dann nämlich feste Regeln für das Ausfüllen aufgestellt werden (keine ungebräuchlichen Abkürzungen, Aktenzeichen angeben, wenn vorhanden usw.), die die Abfrageberechtigung transparent machen.

Wir sind der Auffassung, dass das derzeitige System der Zugriffsprotokollierungen verschiedene Voraussetzungen erfüllen muss, um dem Grundsatz der Revisionsfähigkeit zu entsprechen:

- Die Angaben in den Abfragemasken müssen einen Rückschluss darauf ermöglichen, ob eine Datenabfrage rechtmäßig war. Es bedarf einer verbindlichen Ver-

pflichtung zur Ausfüllung der Abfragemaske, und es muss sicher gestellt werden, dass die Verbindlichkeit, die Maske auszufüllen, nur in Eilfällen entfällt.

- Nicht oder unzureichend ausgefüllte Abfragemasken müssen statistisch dokumentiert werden.
- Es muss eine statistische Auswertung erfolgen, die erkennen lässt, wie die Kontrolleure die Zugriffe bewerten. Dies kann etwa durch ein (automatisiert bereit gestelltes) Formular erfolgen, auf dem die Kontrolleure die Rechtmäßigkeit des Zugriffs beurteilen.
- Es muss dokumentiert werden, in wie vielen Fällen welche Maßnahmen ergriffen wurden.
- Erledigte Kontrollmitteilungen müssen in einer gesicherten Umgebung so aufbewahrt werden, dass sie einer zusätzlichen Überprüfung, etwa durch unsere Behörde, zugänglich sind.
- Die unbegrenzt mögliche Delegation der Durchführung der Stichprobenkontrollen auf Vorgesetzte niedrigerer Dienstgrade sollte begrenzt werden. Denn sonst besteht die Gefahr, dass Vorgesetzte sich aufgrund ihrer unmittelbaren Zusammenarbeit mit Kollegen scheuen, den Stichproben hinreichend nachzugehen und gegebenenfalls Maßnahmen gegen ihre Kollegen zu ergreifen.

Wir werden die Wirksamkeit des Stichprobenverfahrens und seine Überprüfbarkeit künftig im Auge behalten. Denn solange das Stichprobenverfahren nicht überprüfbar ist und keine Rückschlüsse auf seine Effizienz zulässt, wirft es nicht nur Fragen nach seiner Wirtschaftlichkeit auf, sondern ist auch die datenschutzrechtliche Revisionsfähigkeit des Verfahrens, die §8 HmbDSG fordert, nicht sicher gestellt.

4.6 Elektronisches Verwahrbuch

Im Januar 2008 trat die Polizei Hamburg mit dem Anliegen an uns heran, mit dem „Elektronischen Verwahrbuch" (EVB) die digitale Verwaltung in Gewahrsam genommener Personen und verwahrter Sachen kurzfristig einzuführen.

Zweck des EVB soll sein, die revisionssichere Dokumentation aller Maßnahmen im Zusammenhang mit der Verwahrung von Personen und Gegenständen zu gewährleisten, damit polizeiliche Maßnahmen auch im Nachhinein detailliert nachvollzogen werden können. Neben Personendaten sollen Angaben über Datum und Uhrzeit von Ereignissen und über den Zustand von Personen oder Sachen festgehalten werden. Zugleich will die Polizei mit dem EVB einer Forderung des Rechnungshofes aus dem Jahr 2002 nachkommen. Die bestehende „Asservatenverwaltung" soll in das EVB integriert werden.

Zum EVB bzw. zur Risikoanalyse und Verfahrensbeschreibung hatten wir einige Fragen und Anregungen. Unter anderem fehlten, wie in anderen, uns vorgelegten Verfahren auch, Vereinbarungen mit Auftragnehmern nach §3 Hamburgisches Datenschutzgesetz (HmbDSG). Ebenso fehlte eine vertragliche Vereinbarung mit dem Dienstleister Dataport über ergänzende Schutzmaßnahmen für Daten mit hohem Schutzbedarf.

In einer ausführlichen Stellungnahme der IuK-Abteilung vom September 2008 wurden einige Anregungen aufgenommen und offene Fragen geklärt. Wir konnten erreichen, dass die unterschiedslose Speicherdauer von 5 Jahren ersetzt wurde durch eine differenzierte Speicherfrist. Bei Ingewahrsamnahmen und Freiheitsbeschränkungen wurde die Frist auf 2 Jahre gesenkt; eine 5-jährige Speicherdauer ist

nur für Festnahmesachen vorgesehen. Nach Fristablauf werden die Daten automatisch gelöscht. Im Juli 2009 wurden uns die überarbeiteten Fassungen der Risikoanalyse und der Verfahrensbeschreibung überlassen. Angaben, durch welche technisch-organisatorischen Maßnahmen dem hohen Schutzbedarf genügt wird, bzw. notwendige vertragliche Vereinbarungen mit dem Dienstleister Dataport und mit den Auftragnehmern, stehen jedoch noch aus.

4.7 Videoüberwachung im Schanzenviertel

Videoüberwachung zum Zwecke strafrechtlicher Ermittlungen richtet sich nach der Strafprozessordnung; technisch-organisatorische Sicherheitsmaßnahmen hat auch der Hamburgische Datenschutzbeauftragte zu bewerten.

Anfang Juni 2009 berichtete die Presse, dass die Polizei im Schanzenviertel private Geschäftsinhaber auffordere, zu ihrem Schutz Videokameras aufzustellen. Aber auch von „heimlichen Filmaufnahmen der Polizei in der Schanze" war die Rede. Da hier sehr verschiedene rechtliche Bewertungen in Betracht kamen – private Videoüberwachung des öffentlichen Raums, (präventive) polizeiliche Videoüberwachung zur Gefahrenabwehr und (repressive) Videoaufnahmen zur Aufklärung einer Straftat – erbaten wir von der Polizei Aufklärung. Diese teilte mit, es gehe ausschließlich um eine strafprozessuale Maßnahme: Wegen erwarteter Wiederholungstaten zeichnete in den Nachtstunden eine Videokamera im Geschäftsraum eines Opfers die Situation vor dem Geschäft auf. Erst später wurden wir nach weiteren Rückfragen darüber informiert, dass noch ein weiterer Ort durch mehrere Videokameras beobachtet wurde.

Aufgrund einer differenzierten Einsatzbeschreibung der Polizei zur erstgenannten Maßnahme und einer Besichtigung des zweiten Beobachtungsobjekts vor Ort konnten wir die strafprozessuale Zielrichtung der Videoüberwachung nachvollziehen. Damit richtete sich die Maßnahme hinsichtlich Anlass, Zielobjekt, Verhältnismäßigkeit, Datenkennzeichnung, späterer Benachrichtigung der Betroffenen und Löschung allein nach den §§ 100h, 101 Strafprozessordnung (StPO). Insofern wird das Hamburgische Datenschutzgesetz durch die bereichsspezifischen Normen der Strafverfolgung verdrängt.

Die StPO regelt jedoch nicht die erforderlichen technisch-organisatorischen Sicherungsmaßnahmen zum Schutz vor einem ungefugten Datenzugriff durch Dritte. Hier wiesen wir auf Verbesserungsmöglichkeiten hin. Daraufhin wurde das Kassettenfach der eingesetzten Videokamera versiegelt. Wie schon im Rahmen der präventiv-polizeilichen Videoüberwachungen (21. TB, 8.2) blieben zwischen Polizei und uns grundsätzliche Meinungsverschiedenheiten zu der Frage, ob es sich bei der analogen oder digitalen Videobeobachtung und Bildaufzeichnung um ein „automatisiertes Verfahren" handelt – ob also Vorabkontrolle und Verfahrensbeschreibung erforderlich sind.

Wir nahmen die zunehmende öffentliche Diskussion über Videoüberwachungen im öffentlichen Raum – durch Wirtschaft und Staat – zum Anlass, die Frage des „automatisierten Verfahrens"" gerade auch aus technischer Sicht noch einmal breit in der Dienststelle zu diskutieren. Wir kamen zu dem Ergebnis, dass nicht nur digitale, sondern auch analoge Videokameras zusammen mit den modernen Möglichkeiten der Bildauswertung auf speziellen Recordern mit spezialisierter Software heute als „automatisierte Verfahren" im Sinne des Datenschutzrechts angesehen werden müssen. Anderslautende Meinungen in einem Teil der Kommentarliteratur konnten uns nicht überzeugen.

Im November 2009 konnten wir uns in einem Gespräch mit der Polizei für den besonderen Fall der Videoüberwachung zu Ermittlungszwecken auf Folgendes einigen: Staatsanwaltschaft und Polizei entscheiden über den konkreten Einsatz verdeckter Videokameras nach der StPO grundsätzlich ohne Beteiligung des Datenschutzbeauftragten. Zur Beurteilung der Datensicherheit der eingesetzten Systeme stellt uns die Polizei entsprechende Unterlagen zu den typischerweise eingesetzten Systemen und in bestimmten Intervallen eine Übersicht über die Anzahl der Einsätze zur Verfügung. Wir bieten der Polizei allgemeine Hinweise zu technisch-organisatorischen Sicherheitsmaßnahmen beim Einsatz der Videosysteme an. In besonderen Fallkonstellationen soll es einen Austausch über die vom Normalfall abweichenden Umstände und etwaige Folgerungen für die Datensicherheit geben.

5. Verfassungsschutz

5.1 Erfassung von Personen, die Infostände anmelden

Unsere Intervention beim Landesamt für Verfassungsschutz (LfV) und bei den Bezirken trug wesentlich dazu bei, dass das LfV seine Aufforderung an die Bezirke zurücknahm, die Personalien aller Infostand-Anmelder zu übermitteln.

Im Oktober 2008 hatte das LfV die Bezirke schriftlich gebeten, ihm regelmäßig Namen, Adresse und Organisation jeder Person zu übermitteln, die eine Sondernutzungserlaubnis für einen Informationsstand beantragt. Die Medien und eine Kleine parlamentarische Anfrage griffen das auf und offenbarten, dass in Hamburg jährlich mehr als 3000 Infostände vornehmlich von Parteien, aber auch von Hilfsorganisationen und Initiativen angemeldet werden.

Ohne vorher vom LfV angesprochen worden zu sein, teilten wir diesem im November unsere Rechtsauffassung mit: Die allgemeine Aufforderung an die Bezirke verstößt gegen das Verfassungsschutzgesetz, das eine Datenerhebung nur dann rechtfertigt, wenn sie zur Erfüllung der Aufgaben des LfV erforderlich ist. Die Aufgaben des LfV beziehen sich ausdrücklich auf die Bekämpfung von Bestrebungen gegen die freiheitliche demokratische Grundordnung und von sicherheitsgefährdenden Tätigkeiten. Wir forderten deswegen für eine Datenübermittlung aus den Bezirksämtern zumindest Anhaltspunkte dafür, dass der angemeldete Infostand bzw. die anmeldende Organisation solcher Handlungen verdächtig ist. Im Übrigen verwiesen wir darauf, dass die Bezirksämter nur bei besonders gefährlichen Organisationen zur Übermittlung an das LfV verpflichtet, ansonsten nur dazu „befugt" sind. Dieses teilten wir in gleichlautenden Schreiben allen Bezirksamtsleiterinnen und -leitern mit.

In seiner Antwort vom Dezember vertrat das LfV die Meinung, es müsse selbst alle Anmeldungen daraufhin überprüfen, welche von ihnen verfassungsschutz-relevant sind. Auf eine regelmäßige Übermittlung verzichtete das LfV jedoch in Zukunft. Vielmehr würden LfV-Mitarbeiter die Vorgänge von Zeit zu Zeit in den Bezirksämtern sichten.

Parallel hielten wir Kontakt zu den Bezirksämtern. Im März 2009 beschlossen die bezirklichen Rechtsamtsleiter, sich der Meinung des Hamburgischen Datenschutzbeauftragten anzuschließen und Unterlagen zu Infostand-Anmeldungen nicht prüfungslos an das LfV herauszugeben. In Zukunft bitten die Bezirke die sie besuchenden Mitarbeiter des LfV um eine vorherige Festlegung, welche Organisationen oder Akten von besonderem verfassungsrechtlichen Interesses sind. Nur diese werden

dann dem LfV zur Sichtung vorgelegt. Dies ist datenschutzrechtlich nicht zu beanstanden.

5.2 Erkenntnisse und Einbürgerungen

Nicht immer erscheint die Übermittlung von Erkenntnissen des Landesamts für Verfassungsschutz (LfV) an die Einbürgerungsbehörde geeignet und damit erforderlich zur Ablehnung eines Einbürgerungsantrages.

Bereits im 21. TB, Ziff. 9.2 hatten wir davon berichtet, dass Erkenntnisse des LfV für die Betroffenen erhebliche Konsequenzen haben können, obwohl die Schlussfolgerungen, die aus den Erkenntnissen gezogen werden, sich nicht immer aufdrängen und nicht mit den Betroffenen geklärt werden.

Im Berichtszeitraum versuchten wir, in zwei Fällen anhand der Unterlagen des LfV nachzuvollziehen, warum die Anträge der Betroffenen auf Einbürgerung abgelehnt wurden. Die Betroffenen hatten sich an uns gewandt, weil die Ablehnungen mit einer Mitteilung des LfV begründet wurden und ein entsprechendes Auskunftsbegehren beim LfV aus Sicherheitsgründen (Quellenschutz) nur unvollständig beantwortet wurde. Wir können die Unterlagen des LfV einsehen, der betroffenen Person aber nur über das Ergebnis (datenschutzrechtliche Mängel oder Mangelfreiheit) Auskunft geben.

Es kann nicht Aufgabe des Datenschutzbeauftragten sein, sich mit einer eigenen verbindlichen Bewertung von Erkenntnissen an die Stelle des LfV zu setzen. Er kann jedoch seine Meinung äußern, wenn er Zweifel daran hat, dass die übermittelten Daten eine Ablehnung eines Einbürgerungsantrages rechtfertigen. Es geht hier nicht zuletzt um Eignung und Erforderlichkeit der Datenübermittlung.

In einem Fall war der Betroffene auch in jüngerer Zeit bei Veranstaltungen einer extremen islamistischen Organisation beobachtet worden, die vom Verfassungsschutzbericht 2008 als doktrinäre, gewalttätige und aggressive Vereinigung beschrieben und deren Betätigung bundesweit verboten wurde. Im anderen Fall erfuhr das LfV, dass der Betroffene vor nicht langer Zeit Leitungsfunktionen in Unterorganisationen der Türkischen Kommunistischen Partei / Marxisten-Leninisten (TKP-ML) übernommen hatte.

Nach dem Staatsangehörigkeitsgesetz ist Voraussetzung für eine Einbürgerung – neben anderen -, dass die betroffene Person keine Bestrebungen unterstützt (hat), die sich gegen die freiheitliche demokratische Grundordnung der Bundesrepublik richtet oder die die auswärtigen Belange der Bundesrepublik durch die Anwendung oder Unterstützung von Gewalt gefährdet. Eine Einbürgerung ist ausgeschlossen, wenn „tatsächliche Anhaltspunkte die Annahme rechtfertigen", dass die betroffene Person entgegen ihrer Erklärung solche Bestrebungen doch unterstützt (hat).

Im ersten Fall erscheint es plausibel, dass die Teilnahme an den verbotenen Veranstaltungen eine Bestrebung unterstützt, die sich sowohl gegen die freiheitliche demokratische Grundordnung in der Bundesrepublik richtet als auch deren auswärtige Belange durch die Propagierung von Gewalt gefährdet.

Im zweiten Fall bleibt jedoch zweifelhaft, ob die übermittelten Erkenntnisse die genannten „Anhaltspunkte" darstellen. Der Verfassungsschutzbericht 2008 nennt die TKP-ML zwar eine links-extreme Organisation. Ihre Aktivitäten in der Bundesrepublik beschränken sich nach dem Bericht aber im Wesentlichen auf legale Kundgebungen und Demonstrationen zu türkischen Themen. Gewalt unterstützen die

TKP-ML und ihre Unterorganisationen weder in der Bundesrepublik noch in der Türkei. Die auswärtigen Belange der Bundesrepublik scheinen uns zumindest nicht in der vom Staatsangehörigkeitsgesetz geforderten Intensität gefährdet. Wir haben das LfV auf unsere Zweifel an der Erforderlichkeit der Erkenntnisübermittlung in diesem Einzelfall hingewiesen.

Für den Fall, dass das LfV seine bereits übermittelten Erkenntnisse im Nachhinein entscheidend verändert oder löscht, drangen wir darauf, dass dies auch der Einbürgerungsbehörde und dem Betroffenen, der zuvor Auskunft erhalten hatte, nachgemeldet wird. In einem dritten Fall war dies unterblieben, so dass der betroffene Ausländer trotz einer neuen günstigeren Sachlage, nicht eingebürgert wurde, weil die Einbürgerungsbehörde von der Löschung der Erkenntnisse keine Kenntnis hatte.

6. Justiz

6.1 Die neuen Justizvollzugsgesetze

In der Abstimmung der Entwürfe zum Strafvollzugsgesetz, Jugendstrafvollzugsgesetz und Untersuchungshaftvollzugsgesetz konnten sich viele unserer Anregungen und Einwände durchsetzen, andere – auch grundsätzlicher Art – nicht.

Im November 2008 erhielten wir den ersten Entwurf für ein Strafvollzugsgesetz und ein Jugendstrafvollzugsgesetz zur Stellungnahme. In dem am 14. Juli 2009 von der Bürgerschaft beschlossenen Gesetzestext werden folgende unserer Anregungen berücksichtigt:

- Nicht überwacht wird nun auch Post, die der bzw. die Gefangene an Gerichte, Staatsanwaltschaft und Aufsichtbehörde richtet.
- Korrespondenz der Gefangenen mit externen Ärztinnen und Ärzten darf nur durch die anstaltsinternen Ärztinnen und Ärzte überwacht werden.
- Bei den zugelassenen erkennungsdienstlichen Maßnahmen gilt hinsichtlich der Erfassung biometrischer Merkmale nun eine Konkretisierung und Beschränkung auf Finger- und Handabdruck, Gesichts- und Stimmmerkmale. Ferner werden die zu unbestimmten „Messungen" auf Körpermessungen eingegrenzt.
- Für die Errichtung von überregionalen Datenverbünden enthält das Gesetz nun die notwendige Verordnungsermächtigung mit den Bestimmungen über die zu regelnden Inhalte.
- In den „Schutz besonderer Daten" sind nun auch solche aus psychologischen Untersuchungen – neben den aus ärztlichen Untersuchungen – einbezogen.
- Die mögliche Offenbarung von Gesundheitsdaten von Gefangenen gegenüber der Anstaltsleitung ist nun auf die „in der Anstalt tätigen" Ärztinnen und Ärzte beschränkt.

Nicht durchsetzen konnten wir uns vor allem mit folgenden Vorschlägen:

- Verzicht auf eine Videoüberwachung in Funktionsräumen (z.B. Arbeits- und Aufenthaltsräumen), in denen sich regelmäßig mehrere Personen aufhalten,
- Verzicht auf eine verdeckte Videoüberwachung im „Gebäudeinneren" (außer in Hafträumen). Eine verdeckte Überwachung halten wir angesichts des besonderen Gewaltverhältnisses in Justizvollzugsanstalten grundsätzlich für eine unverhältnismäßige Maßnahme. Ihre Eignung und Erforderlichkeit z.B. zur Verhinderung von Ausbruchsversuchen und Drogenmissbrauch erscheint fraglich. Eine offene Überwachung wäre ein geringerer Eingriff mit einer ähnlichen Erfolgs-

aussicht. Die Rechtfertigung der verdeckten Videoüberwachung – „wenn dies zur Aufrechterhaltung der Sicherheit und Ordnung der Anstalt unerlässlich ist" – ist weit und unbestimmt gefasst und trägt dem Grundrechtsschutz nach unserer Auffassung nur unzureichend Rechnung.

Ab Juli 2009 wurde auch der Entwurf eines Hamburger Untersuchungshaftvollzugsgesetzes zwischen den Behörden abgestimmt. Einzelne unserer Anregungen wurden übernommen – z.B. dass bei der Aufnahme in der U-Haftanstalt Dritte nur mit Einwilligung des Untersuchungshäftlings anwesend sein dürfen und dass die Löschungsfristen für Unterlagen und Daten in Dateien gleich sein sollten. Streitig blieb einerseits das schon beim Strafvollzugsgesetz diskutierte Thema „verdeckte Videoüberwachung". Andererseits machten wir Einwände geltend gegen die – im Verhältnis zu Strafgefangenen – erweiterte Telefonüberwachung, gegen die unklare Bestimmung zur körperlichen Untersuchung und gegen die Zusammenarbeitsregelungen. Bei letzteren besteht zwar Einigkeit, dass sie die spezialgesetzlichen Datenverarbeitungsbestimmungen etwa im Sozialgesetzbuch nicht verdrängen und auch im übrigen keine Datenverarbeitungsermächtigungen konstituieren können. Den nicht juristisch geschulten Anwender lädt der Gesetzestext jedoch zu Missverständnissen geradezu ein.

6.2 Datenschutz in der Bewährungshilfe

Die Schweigepflicht der Bewährungshelfer und -helferinnen steht den Auskunftswünschen von Arbeitsagentur, Justizvollzug und anderen Behörden meist ebenso entgegen wie dem Bedürfnis der Bewährungshilfe, im Einzelfall das Jugendamt oder die Familie des betroffenen Probanden zu informieren.

Seit Ende 2008 diskutieren die Landes- und Bundesdatenschutzbeauftragten untereinander und mit den Justizbehörden die Frage, ob und in welchem Ausmaß Bewährungshelferinnen und Bewährungshelfer als Sozialarbeiter und Sozialpädagogen der besonderen Schweigepflicht nach § 203 Abs. 1 Nr. 5 Strafgesetzbuch unterliegen. Weitgehende Einigkeit besteht inzwischen darin, dass der klare Wortlaut dieser Vorschrift keine einschränkenden Auslegungen zulässt. Erörtert wird, ob die allgemeinen Datenschutzgesetze und die Amtshilfevorschrift des Grundgesetzes gesetzliche „Befugnisnormen" zur Durchbrechung der Schweigepflicht darstellen.

In mehreren Stellungnahmen und einer Fortbildungsveranstaltung für die Hamburger Bewährungshelferinnen und -helfer haben wir im Einzelnen folgende Positionen vertreten:

Die Schweigepflicht nach § 203 Abs. 1 Nr. 5 StGB gilt für alle Bewährungshelferinnen und helfer mit einer Sozialarbeiter- oder Sozialpädagogen-Ausbildung, obwohl die Bewährungshilfe neben der Unterstützung des Probanden auch hoheitliche Kontrolle über die Einhaltung der Bewährungsauflagen ausübt.

Nach dem Volkszählungsurteil des Bundesverfassungsgerichts bedarf die Durchbrechung dieser Schweigepflicht einer bereichsspezifischen gesetzlichen Ermächtigung. Das StGB gewährt eine Übermittlungsbefugnis nur zwischen der Bewährungshilfe und dem Gericht sowie im Rahmen der Führungsaufsicht zwischen Bewährungshilfe, Gericht, Aufsichtsstelle und forensischer Ambulanz. Der Amtshilfegrundsatz kann dies nicht erweitern. Nur zur Abwendung einer gegenwärtigen Gefahr, also im „Notfall", ist eine Durchbrechung der Schweigepflicht durch Weitergabe von Probandendaten gerechtfertigt, wenn zuvor die kollidierenden Interessen und Pflichten gewissenhaft miteinander abgewogen wurden.

Das Hamburgische Datenschutzgesetz (HmbDSG) schließt eine Datenübermittlung öffentlicher Stellen (hier: der Bewährungshilfe) an private Dritte – wie z.B. die Partnerin des Probanden – angesichts der Schweigepflicht ausdrücklich aus. Die Datenweitergabe an andere Behörden wie Polizei, Justizvollzugsanstalt, Arbeitsagentur (Arge) oder Ausländerbehörde lässt das HmbDSG zu, wenn „hierdurch erhebliche Nachteile für das Gemeinwohl oder schwer wiegende Beeinträchtigungen von gewichtigen Rechtspositionen einzelner verhindert oder beseitigt werden sollen" oder sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zum Vollzug von Strafen oder zur Beantwortung eines gerichtlichen Auskunftsersuchens erforderlich ist. Diese Übermittlungsermächtigung wird jedoch wieder ausgeschlossen, wenn die übermittelnde Behörde die Daten von einer schweigepflichtigen Person in deren Berufsausübung erhalten hatte. Nicht ausdrücklich geregelt ist die Konstellation, dass die Behörden-Mitarbeiter unmittelbar selbst schweigepflichtig sind. Der Sinn der gesetzlichen Regelung – nämlich der Ausschluss einer Weitergabe von Daten, die einem Berufsgeheimnis unterliegen – ist jedoch nur dadurch einzuhalten, dass auch in diesen Fällen eine Übermittlung von Bewährungshelfern an andere Behörden nicht erfolgt. Damit bleibt es grundsätzlich bei der Schweigepflicht.

Häufig werden Bewährungshelferinnen und -helfer auch als Zeugen in Ermittlungs- und Gerichtsverfahren befragt. In Zivil- und Verwaltungsgerichtsprozessen steht ihnen jedoch ein Zeugnisverweigerungsrecht zu, da ihnen kraft Amtes Tatsachen anvertraut werden, deren Geheimhaltung geboten ist. Angesichts ihrer Schweigepflicht nach dem StGB müssen die Bewährungshelferinnen und -helfer von diesem Recht auch Gebrauch machen – es sei denn, der Proband selbst entbindet sie davon.

In Verfahren nach der Strafprozessordnung gibt es dagegen kein Zeugnisverweigerungsrecht für Sozialpädagogen und Sozialarbeiterinnen und -arbeiter. Hier müssen die Bewährungshelferinnen und -helfer jedenfalls vor der Staatsanwaltschaft und dem Gericht auch von ihren Wahrnehmungen zu den Probanden berichten. Allerdings kann der Dienstherr der Bewährungshelfer, der die Zeugenaussage zu genehmigen hat, dies zum Schutz des Bediensteten verhindern. Auch soweit Bewährungshelfer nicht als Zeuge vernommen werden, sondern im Rahmen von Strafermittlungen von der Polizei um Auskunft gebeten werden (§§ 161, 163 StPO), sind sie mangels Zeugnisverweigerungsrecht als Behörde auskunftspflichtig.

Zusammengefasst: Der Gesetzgeber normiert eine enge Kommunikationsbeziehung der Bewährungshilfe allein zu dem Strafgericht, das die Bewährung beschlossen und den Bewährungshelfer bestellt hat, sowie eine Offenbarungspflicht innerhalb von Straf(ermittlungs)verfahren; im Übrigen werden die Interessen der Probanden jedoch grundsätzlich durch die Schweigepflicht der Bewährungshelfer geschützt.

7. Soziales

7.1 Über 500.000 Sozialdatensätze wurden nicht gelöscht

Bei drei IT-Verfahren der Jugend- und Sozialämter wurde ein massiver Verstoß gegen die gesetzlich festgeschriebene Löschungsverpflichtung festgestellt. Der Mangel wurde Ende 2009 behoben.

Im Rahmen einer Prüfung des IT-Verfahrens PROJUGA, mit dem die Sachbearbeitung in den Jugendämtern der Bezirke unterstützt wird, wurden wir darauf aufmerk-

sam, dass seit der Inbetriebnahme des Verfahrens vor ca. 13 Jahren noch kein einziger Datensatz gelöscht wurde, obwohl die Aufbewahrungsfrist zum Teil schon seit Jahren erreicht war. Insoweit wurde gegen die Regelung des § 84 Abs. 2 SGB X verstoßen, wonach Sozialdaten zu löschen sind, wenn ihre Kenntnis für die rechtmäßige Aufgabenerfüllung der speichernden Stelle nicht mehr erforderlich ist.

Aufgabenbereiche wie z.B. die Einrichtung von Amtsvormundschaften und Pflegschaften sowie die Gewährung von Hilfen zur Erziehung und die Gewährung von Leistungen nach dem Unterhaltsvorschussgesetz arbeiten mit PROJUGA. Das zeigt, dass sehr sensible Daten verarbeitet werden. Seit 2006 werden auch die Meldungen zu möglichen Kindeswohlgefährdungen mit PROJUGA verwaltet.

Der Fachlichen Leitstelle, die zur Abteilung IT-Angelegenheiten der Bezirksverwaltung (N/ITB) gehört, war dieser Mangel seit Jahren bekannt. Seit 2002 wurde auch mit größeren Unterbrechungen an einem Konzept zur Löschung gearbeitet. Im Auftrag der Fachlichen Leitstelle hat Dataport im März 2006 ein umfangreiches Konzept vorgelegt. Die Realisierung des Löschkonzepts unterblieb jedoch, weil immer wieder aktuelle Anpassungen an dem Verfahren vorgenommen wurden, so dass die gesetzlich vorgeschriebene Löschung der nicht mehr erforderlichen Daten in Abstimmung zwischen der Fachlichen Leitstelle und dem fachlich federführenden Bezirk immer wieder zurückgestellt wurde.

Anfang 2009 legte N/ITB darüber hinaus offen, dass auch in den IT-Verfahren zur Unterstützung der Sozialhilfesachbearbeitung (PROSA) und der Wohngeldsachbearbeitung (DIWOGE) seit der jeweiligen Inbetriebnahme Anfang bzw. Mitte der 90iger Jahre noch keine Datensätze gelöscht wurden. Eine erste Abschätzung, die von der Fachlichen Leitstelle auf unser Drängen vorgenommen wurde, machte schnell das immense Ausmaß des Mangels deutlich. In den drei IT-Verfahren waren über 560.000 Datensätze nicht gelöscht worden, obwohl die Löschungsfrist erreicht war.

Tabelle: Übersicht über die Anzahl zu löschender Datensätze und den Löschstatus

IT-Verfahren	Personen im Bestand	Löschbare Personen	Löschstatus (Vorwiegend einfache Fälle) zum 30.06.2009	Löschstatus (incl. komplexe Fälle) zum 30.11.2009
PROJUGA	366.193	104.212	85 %	100 %
PROSA	1.580.000	333.286	84 %	100 %
DIWOGE	487.000	128.639	89 %	100 %
Gesamt	2.433.193	566.137	85 %	100 %

Während bei den Verfahren PROSA und DIWOGE diese Datensätze wenigstens gesperrt, also dem Zugriff der normalen Sachbearbeitung entzogen waren, konnten die Datensätze im Verfahren PROJUGA von der Sachbearbeitung genauso eingesehen werden, wie die aktuell benötigten.

Die Fachliche Leitstelle hat in enger Abstimmung mit uns nach einer eingehenden Erörterung der Missstände eine detaillierte Planung für die Realisierung des Löschens erstellt. Es wurden Meilensteine fest verabredet, um zu verhindern, dass erneut die Realisierung des Löschens aufgrund anderer Anpassungsaktivitäten

zurückgestellt wird. Aufgrund der Priorisierung und des großen Einsatzes aller Beteiligten konnten die festgelegten Termine erreicht werden, so dass zum 30. Juni 2009 insgesamt ca. 480.000 Datensätze gelöscht wurden. Die verbliebenen Datensätze konnten zu diesem Zeitpunkt noch nicht vollständig gelöscht werden, da sie sich mit Personen in Wohn- und Wirtschaftsgemeinschaften bzw. Bedarfsgemeinschaften befanden, deren Vernichtungsdatum noch nicht abgelaufen war. Für diese komplexen Fälle wurde mittlerweile ebenfalls ein Löschkonzept erstellt. Dieses wurde zum 30. November 2009 vollständig umgesetzt, so dass damit einerseits der gravierende Mangel aus der Vergangenheit behoben ist und andererseits sichergestellt sein wird, dass zukünftig eine Löschung fristgerecht entsprechend der festgeschriebenen Löschungsfristen erfolgen wird.

7.2 Baualtersklassennachweis bei SGB II-Leistungen

Es ist nicht immer erforderlich, den Vermieter bei der Bestimmung der Baualtersklasse einer Wohnung zu beteiligen.

Bei der Bewilligung von „Leistungen für Unterkunft und Heizung" nach § 22 SGB II handelt es sich um kommunale Leistungen. Deshalb hat die Behörde für Soziales, Familie, Gesundheit und Verbraucherschutz (BSG) im Hinblick auf ein Urteil des Bundessozialgerichts zur Angemessenheit der Unterkunftskosten, wonach der Wohnungsstandard am konkreten Wohnort zu berücksichtigen ist, in einer Fachanweisung zu § 22 SGB II Höchstwerte zu den Kosten der Unterkunft festgelegt. Ein wesentliches Merkmal ist dabei die Bestimmung der Baualtersklasse der Wohnung.

Die Beurteilung der Baualtersklasse erfolgt durch das Jobcenter in der Regel nach dem Baujahr bzw. der Bezugsfertigkeit der Wohnung. Um- und Ausbau sowie Modernisierungen haben gegebenenfalls eine „Verjüngung" der Baualtersklasse zur Folge. Für den Fall, dass der Empfänger von Arbeitslosengeld II nicht über die notwendigen Angaben über seine Wohnung verfügt, wird ihm ein Vordruck „Nachweis der Baualtersklasse" mit der Bitte, die entsprechenden Nachweise des Vermieters einzuholen, vom Jobcenter ausgehändigt.

Mehrere Betroffene haben sich bei uns über diese Praxis beklagt. Sie waren vom Jobcenter aufgefordert worden, das Formular von ihrem Vermieter oder Hausverwalter ausfüllen zu lassen, ohne auf die Möglichkeit alternativer Datenrecherche hingewiesen worden zu sein. Nachdem wir dies moniert hatten, haben die Jobcenter die Hilfeempfänger darauf hingewiesen, dass die formularmäßige Bestätigung des Vermieters über die Baultersklasse nur benötigt wird, wenn ansonsten keine entsprechenden Unterlagen vorgelegt werden können. Sofern sich die Baualtersklasse des Mietobjektes nicht bereits aus dem Mietvertrag ergibt, könnten die entsprechenden Angaben beispielsweise in einem Mieterhöhungsschreiben enthalten sein.

Dieses Ergebnis war datenschutzrechtlich nur halbwegs zufriedenstellend. Denn in den Fällen, in denen der Vordruck „Nachweis der Baualtersklasse" beim Vermieter vorgelegt werden muss, erfährt dieser möglicherweise zum ersten Mal, dass sein Mieter Leistungen nach dem SGB II erhält. Dies könnte durchaus zukünftig das Mietverhältnis belasten. Besonders problematisch war, dass von dem Hilfeempfänger verlangt wurde, sein Vermieter möge ihm eine Bestätigung der Gebäudeversicherung über die Sanierung und Modernisierung des Gebäudes vorlegen.

Nachdem wir erfahren hatten, dass es in anderen Bundesländern durchaus möglich ist, die Baualtersklasse regelmäßig ohne Beteiligung des Vermieters zu ermitteln, haben wir die BSG aufgefordert, dies auch in Hamburg zu realisieren. Die intensiven Beratungen zwischen uns und der BSG konnten kurz vor Redaktionsschluss lediglich mit einem Zwischenergebnis abgeschlossen werden.

Der Vordruck „Baualtersklassennachweis" wird vom Mieter selbst ausgefüllt und unterzeichnet. Allerdings müssen dann zusätzlich Belege beigebracht werden, die geeignet sind, die vollständige Modernisierung durch den kommunalen Leistungsträger zweifelsfrei nachzuweisen. Für den Fall, dass der Mieter keine Nachweise vorlegen kann, verlangt die BSG nach wie vor, dass der Vordruck dem Vermieter vorgelegt wird. Unterschreibt der Vermieter den Vordruck, genügt diese Erklärung als Nachweis für die Modernisierungsmaßnahmen. Der Nachweis der Gebäudeversicherung soll lediglich noch als Beispiel für geeignete Nachweise aufgeführt werden, eine verpflichtende Vorlage ist damit jedoch nicht mehr verbunden.

Obwohl dieses Ergebnis ein weiterer datenschutzrechtlicher Fortschritt ist, dauert die Diskussion mit der BSG über eine Praxis, die wir mittragen können, noch an. Insbesondere wird es darauf ankommen, in welcher Form die Betroffenen über das Verfahren aufgeklärt werden und wie der neue Vordruck „Baualtersklassennachweis" konkret aussehen wird. Die BSG hat zugesagt, beides vor der endgültigen Umsetzung mit uns abzustimmen.

7.3 Rundfunkgebührenbefreiung für Hartz IV-Empfänger

Endlich ist das Verfahren den datenschutzrechtlichen Erfordernissen angepasst worden.

Am 1. September 2008 ist in Hamburg der Zehnte Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge (Zehnter Rundfunkstaatsänderungsvertrag) in Kraft getreten, mit dem auch §6 Abs. 2 des Rundfunkgebührenstaatsvertrages (RGebStV) geändert wurde. Danach kann der Empfänger von Sozialleistungen jetzt wählen, wie er gegenüber der Gebühreneinzugszentrale (GEZ) nachweist, dass er die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht erfüllt. Bisher war er gehalten, der GEZ den gesamten Leistungsbescheid im Original oder zumindest in beglaubigter Kopie vorzulegen. Dadurch wurden der GEZ weit mehr Daten übermittelt, als sie für die Entscheidung über den Antrag auf Rundfunkgebührenbefreiung benötigte. Jetzt kann der Empfänger von Sozialleistungen vom Leistungsträger eine gesonderte Bescheinigung verlangen, aus der hervorgeht, dass er die Voraussetzungen zur Befreiung von der Rundfunkgebührenpflicht erfüllt. Diese Bescheinigung wird von der GEZ akzeptiert. Weiterhin besteht aber auch die Möglichkeit, den Leistungsbescheid im Original oder in beglaubigter Kopie der GEZ vorzulegen.

In den Job-Centern von team.arbeit.hamburg (Hamburger Arbeitsgemeinschaft SGB II) war diese Änderung nicht von Beginn an hinreichend bekannt. Dies führte dazu, dass sich immer wieder Hartz IV-Empfänger bei uns darüber beschwerten, die Job-Center würden sich weigern, ihnen die begehrte Bescheinigung zur Vorlage bei der GEZ auszustellen. Es handelte sich dabei um einen Vordruck, der ausdrücklich zwischen den Datenschutzbeauftragten des Bundes und der Länder und der GEZ abgestimmt worden war. Nachdem wir mehrfach bei der Geschäftsleitung von team.arbeit.hamburg interveniert haben, erreichen uns inzwischen keine Beschwerden mehr.

Grund dafür dürfte auch sein, dass die Bundesagentur für Arbeit in Nürnberg reagiert hat, nachdem wir gemeinsam mit den anderen Datenschutzbeauftragten der Länder auf eine gesetzeskonforme Anpassung des Verfahrens gedrängt hatten. Zum einen weist sie jetzt in Ihrem Internetauftritt auf die Möglichkeit hin, sich vom Job-Center die Angaben bestätigen zu lassen, die von der GEZ für die Entscheidung über einen Antrag auf Rundfunkgebührenbefreiung benötigt werden. Zum anderen hat die Bundesagentur für Arbeit verfahrensmäßig sichergestellt, dass automatisch jedem Bewilligungs- und Änderungsbescheid eine Bescheinigung zur Vorlage bei der GEZ an die Hartz IV-Empfänger beigefügt wird. Auf der Bescheinigung sind nur die Daten aufgeführt, die die GEZ im Zusammenhang mit dem Befreiungsantrag benötigt, nämlich Name, Vorname, Straße und Wohnort des Leistungsempfängers sowie Bewilligungszeitraum und gegebenenfalls an wen und für welchen Zeitraum Leistungen nach dem SGB II gezahlt werden. Mit dieser Lösung können nicht nur wir, sondern auch die vielen Hartz IV-Empfänger sehr zufrieden sein.

7.4 Übernahme der Kosten einer Klassenreise durch die ARGE

Hartz IV-Empfänger, deren Kinder an einer Klassenreise teilnehmen, werden jetzt nicht mehr anders behandelt als die Eltern anderer Kinder.

Wenn das Kind eines Hartz IV-Empfängers an einer Klassenreise teilnehmen will, können die Eltern die Übernahme der Kosten bei der ARGE beantragen. Bislang entsprach es der gängigen Praxis, dass der entsprechende Betrag von der ARGE auf das Konto des Lehrers überwiesen wurde, der die Klassenreise durchführt. Dadurch erfuhr der Lehrer oftmals zum ersten Mal, dass die Eltern seines Schülers arbeitslos sind. Die ARGE begründete diese Praxis im Wesentlichen damit, dass erfahrungsgemäß das für die Klassenreise vorgesehene Geld nicht selten anders verwendet wird.

Nach §23 Abs. 3 Satz 1 Nr. 3 SGB II sind Leistungen für mehrtägige Klassenfahrten im Rahmen der schulrechtlichen Bestimmungen nicht von der Regelleistung umfasst. Vielmehr handelt es sich um einen Sonderbedarf, für den einmalige Leistungen in Betracht kommen. Sinn und Zweck dieser Bestimmung ist es, eine Ausgrenzung schulpflichtiger hilfebedürftiger Kinder im Verhältnis zu nicht hilfebedürftigen, an der Klassenfahrt teilnehmenden Mitschülern zu vermeiden. Es mag in der Tat Fälle geben, in denen solche Sonderleistungen von den Leistungsempfängern zweckwidrig verwendet worden sind. Dies darf jedoch nicht dazu führen, dass sämtliche Leistungsbezieher sozusagen unter Generalverdacht gestellt werden, sie würden mit den ihnen zustehenden Sonderleistungen nicht zweckgerecht umgehen.

Eine Direktzahlung der Sonderleistung für die Kosten einer Schulfahrt an die Lehrkraft kommt aus unserer Sicht nur dann in Betracht, wenn der ARGE im jeweiligen Einzelfall bereits konkrete Anhaltspunkte vorliegen, dass der Leistungsbezieher die Mittel zweckwidrig verwenden wird. Liegen aber solche Anhaltspunkte nicht vor, sollte einer Auszahlung der Sonderleistung an den Leistungsbezieher nichts im Wege stehen.

Die Verfahrensweise der ARGE richtet sich nach fachlichen Vorgaben der Behörde für Soziales, Familie, Gesundheit und Verbraucherschutz (BSG), da das Geld nicht vom Bund, sondern vom Land zur Verfügung gestellt wird. Wir haben deshalb gegenüber der BSG deutlich gemacht, dass die Handlungsanweisung, nach der sich die ARGE zu richten hat, datenschutzrechtlich bedenklich ist.

Die BSG konnte unsere Rechtsauffassung nachvollziehen und änderte die Fachanweisung. Jetzt muss ein Hartz IV-Empfänger grundsätzlich nicht mehr die Bankverbindung des Lehrers angeben, der die Klassenreise durchführt, sondern das Geld wird dem Hartz IV-Empfänger überwiesen. Lediglich in den Fällen, in denen bereits im Vorwege ein unwirtschaftliches Verhalten der Familie aktenkundig ist und ein Missbrauch der Leistungen befürchtet werden muss, soll das Geld für die Klassenreise auf das Konto des Lehrers überwiesen werden. Zwar erfährt der Lehrer dann nicht nur, dass die Familie Leistungen von der ARGE erhält, sondern auch noch, dass die Familie offensichtlich nicht mit dem Geld umgehen kann. Dies müssen die Betroffenen aber hinnehmen, weil ansonsten die Gefahr besteht, dass bei einer zweckwidrigen Verwendung der Mittel das Kind nicht an der Klassenreise teilnehmen kann. Ein Nachteil, der im Vergleich mit den datenschutzrechtlichen Aspekten schwerer wiegt.

7.5 ELENA: Verfassungsrechtlich umstritten – technisch-organisatorisch verbessert

Die zentrale Speicherung der Entgeltdaten von mehr als 30 Millionen Beschäftigten ist mit dem Grundsatz der Verhältnismäßigkeit nicht vereinbar. Durch ELENA wird ein riesiger Datenpool auf Vorrat geschaffen, bei dem nicht absehbar ist, welche Daten überhaupt jemals benötigt werden. Immerhin konnten in der Vergangenheit zumindest technisch-organisatorische Verbesserungen erreicht werden.

Mit dem bundesweiten IT-Verfahren ELENA werden die Elektronischen Entgelt-Nachweise aller Beschäftigten in Deutschland ab 1. Januar 2010 in einer zentralen Speicherstelle vorgehalten. Für diesen Zweck werden die Arbeitgeber verpflichtet, monatlich die Höhe und Zusammensetzung des Entgelts für jeden Beschäftigten elektronisch an die zentrale Speicherstelle zu melden. Dort werden die Meldungen je nach Bestandteil des Entgeltnachweises bis zu 5 Jahre gespeichert. Wenn Bürgerinnen und Bürger eine Sozialleistung wie z.B. Arbeitslosengeld oder Elterngeld beantragen, für die ein Einkommensnachweis erforderlich ist, soll die zuständige Stelle diesen ab dem 1. Januar 2012 elektronisch von der zentralen Speicherstelle abrufen. Die in der zentralen Speicherstelle gespeicherten Daten werden jedoch nur genutzt, wenn der Betroffene während der Speicherfrist einen Antrag auf Sozialleistungen stellt. Da ein Großteil der Betroffenen innerhalb dieser Zeit keine Sozialleistungen beantragen wird, werden die meisten dort gespeicherten Entgeltmeldungen nach Ablauf der Speicherfrist gelöscht, ohne dass sie genutzt worden sind. Aus diesem Grund haben die Datenschutzbeauftragten des Bundes und der Länder wiederholt rechtliche Bedenken geäußert, weil die Speicherung nicht den Grundsätzen der Verhältnismäßigkeit und der Erforderlichkeit entspricht. Für den Fall, dass diese Bedenken ausgeräumt werden könnten, haben sie umfangreiche technische und organisatorische Schutzmaßnahmen gefordert, die gesetzlich verankert werden müssen. Dazu gehört insbesondere, dass der gewaltige und sehr sensible Datenbestand in der zentralen Speicherstelle nur verschlüsselt gespeichert werden darf. Außerdem haben die Datenschutzbeauftragten verlangt, dass die Verantwortung für diese Ver- und Entschlüsselungskomponente einem unabhängigen Treuhänder übergeben werden muss. Im ELENA-Verfahrensgesetz wurde daraufhin festgeschrieben, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) den Datenbank-Hauptschlüssel verwaltet.

Für die Verschlüsselung der Daten wird ein Hardware Security Modul (HSM) genutzt, das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert ist. Dieses Modul wird zwar beim Betreiber der Zentralen Speicherstelle, der

Deutschen Rentenversicherung Bund, installiert, jedoch verantwortet der BfDI die sichere Aufbewahrung und Verwaltung des Datenbank-Hauptschlüssels, den Schutz des Datenbank-Hauptschlüssels vor unberechtigter Nutzung und die Überwachung und Kontrolle der Abrufmaßnahmen. Der BfDI wirkt bei der Zustimmung zur Realisierung von Änderungen im HSM-Zugriffsmodul mit, gibt die Prozesse frei, die auf das HSM zugreifen und hat das Prüfrecht der Programmversionen. Dazu könnten gegebenenfalls unter Einbindung externer Gutachter auch Code-Reviews durchgeführt werden.

Diese umfangreichen Rechte des BfDI sowie die weiteren geplanten Schutzmaßnahmen tragen dazu bei, dass ein ausreichendes Maß an technologischem Datenschutz sichergestellt ist.

Bevor ab 2012 die Entgeltdaten von den Behörden, die ELENA nutzen dürfen, abgerufen werden, müssen hierfür noch bundesweit einheitliche Mindestanforderungen festgelegt werden. Es ist sichergestellt, dass die Datenschutzbeauftragten an diesen Festlegungen beteiligt werden.

7.6 Gemeinsame Fallkonferenzen über junge Gewalttäter

Bei behördenübergreifenden Fallkonferenzen muss der Informationsfluss an datenschutzrechtlichen Spezialvorschriften ausgerichtet werden.

Der Senat hat im Rahmen seines Projektes „Handeln gegen Jugendgewalt" (Bürgerschaftsdrucksache 18/7296) entschieden, behördenübergreifende gemeinsame Fallkonferenzen über delinquente Jugendliche einzuführen, in denen Informationen über den Jugendlichen und seine aktuelle Entwicklung ausgetauscht werden. Die Teilnehmer der Fallkonferenz sollen Handlungsschritte und Maßnahmen entwickeln, die zu einem gesetzestreuen Verhalten der Jugendlichen führen sollen. An den Fallkonferenzen sind Vertreter der Polizei, der Staatsanwaltschaft und der Jugendhilfe sowie im Einzelfall weiterer Behörden – wie z.B. der Ausländerbehörde – und Institutionen beteiligt.

Die praktische Durchführung der Fallkonferenzen wurde von den beteiligten Behörden konzipiert. Wir wurden nur marginal eingebunden, machten aber beizeiten auf die spezialgesetzlich geregelten Datenübermittlungs- und -verarbeitungsvorschriften aufmerksam, die einen Datenaustausch unter mehreren, gleichzeitig anwesenden Behördenvertretern äußerst engen Grenzen unterwerfen. Insbesondere müssten die in Fallkonferenzen anwesenden Behördenvertreter bei jedem Einzelfall und bei jedem personenbezogenen Datum darüber hinaus das Erforderlichkeitsprinzip beachten – und zwar hinsichtlich jeder einzelnen vertretenen Behörde.

Letztlich wurde der Polizei die Koordinierung und Organisation der Fallkonferenzen übertragen. Dies halten wir für besonders bedenklich, weil damit alle Informationen über die Betroffenen (dies sind vor allem Kinder, Jugendliche, Erziehungsberechtigte und sonstige Bezugspersonen) dort zusammenlaufen.

Den Wunsch, alle verfügbaren Informationen zusammenzuführen, um zu helfen und die Gesellschaft zu schützen, können wir nachvollziehen. Derartige Fallkonferenzen berühren jedoch in erheblichem Maße datenschutzrechtliche Grundpositionen. In den Fallkonferenzen selbst werden durch den Austausch vorbereitender Unterlagen, durch die Erörterungen im Plenum und durch die Erteilung von Zugriffsrechten auf die Sitzungsprotokolle zwischen den beteiligten Behörden sensibelste Daten ausgetauscht.

Wir betrachten dies mit Sorge, denn durch behördenübergreifende gemeinsame Fallkonferenzen darf das Prinzip der „informationellen Gewaltenteilung", das der Zweckbindung personenbezogener Daten innewohnt, nicht außer Kraft gesetzt werden. Dieses Prinzip dient dem Schutz des Betroffenen. Im Bereich Jugendhilfe sichern die restriktiven Bestimmungen zur Datenübermittlung im Sozialgesetzbuch VIII das besondere persönliche Vertrauensverhältnis zwischen Jugendamt, Jugendlichen und Erziehungsberechtigten. Einen solchen Vertrauensschutz zwischen Polizei, Staatsanwaltschaft und Ausländerbehörde einerseits und den Betroffenen andererseits hat der Gesetzgeber in den weit reichenden Übermittlungsbefugnissen dieser Behörden nicht vorgesehen. Prinzipiell sehen wir die Rechtslage so, dass die Jugendämter die geringsten Mitteilungsbefugnisse gegenüber anderen Behörden haben und die Polizei den weitesten Spielraum zur Datenübermittlung hat. Damit passt nicht zusammen, dass bei der Polizei die meisten Erkenntnisse – eben auch die der Jugendämter – zusammenfließen. Deshalb stellen wir uns zumindest vor, dass als koordinierende Stelle für behördenübergreifende Fallkonferenzen das Jugendamt tätig werden sollte, zumal es die sachnächste Stelle für Jugendhilfeangelegenheiten ist.

Wir befürchten, dass die spezialgesetzlichen Regelungen nicht richtig angewendet werden. Dies betrifft z. B. die Erforderlichkeit der Datenübermittlung für die Aufgabenerfüllung der empfangenden Stelle. So wurde teilweise von Datenübermittlungen „an die Fallkonferenz" gesprochen oder es wurden Datenübermittlungen damit gerechtfertigt, dass sie „für das Gelingen der Fallkonferenz" erforderlich seien. Die Fallkonferenz als solche ist jedoch keine Stelle im Sinne des Datenschutzrechts. Weder verschmelzen die beteiligten Behörden durch das Senatskonzept zu einer Stelle, noch ist das Gelingen der Fallkonferenz deren gesetzliche Aufgabe. Dadurch, dass der Senat eine behördenübergreifende Zusammenarbeit bei delinquenten Jugendlichen beschlossen hat, ist das Gelingen einer Fallkonferenz auch nicht gesetzliche Aufgabe der einzelnen beteiligten Behörden geworden. Zudem ist die Abwehr von Kindeswohlgefährdungen originäre Aufgabe der Jugendhilfe, nicht der Polizei. Zwar ist die Abwehr einer Kindeswohlgefährdung eine Maßnahme der Gefahrenabwehr, jedoch ist die Polizei nach § 3 des Gesetzes zum Schutz der öffentlichen Sicherheit und Ordnung (SOG) dazu nur nachrangig in unaufschiebbaren Fällen berufen. Auch erscheint fraglich, ob eine Fallkonferenz, in der unter regelmäßiger Beteiligung der Ausländerbehörde die Möglichkeiten der Abschiebung erörtert werden, überhaupt zur Abwehr einer Kindeswohlgefährdung geeignet sein kann. Insoweit muss das Prinzip der informationellen Gewaltenteilung beachtet werden.

Es darf angesichts mehrerer beteiligter Behörden nicht aus dem Blick geraten, dass eine gesetzlich zulässige Datenübermittlung sozusagen in einer Einbahnstraße zwischen zwei Stellen geschieht. Weder umfasst Datenübermittlung ein Mithören einer dritten Behörde, noch erlaubt sie eine Rückmeldung der empfangenden Stelle.

Die Verarbeitung personenbezogener Daten ist grundsätzlich nur auf gesetzlicher Grundlage oder mit Einwilligung des Betroffenen zulässig. Die an den Fallkonferenzen beteiligten Behörden gingen jedoch häufig von einer mutmaßlichen Einwilligung der Betroffenen aus und leiteten daraus die Zulässigkeit ihres Datenaustauschs ab. Letztlich dürfen die beteiligten Behörden sich nicht auf eine mutmaßliche Einwilligung berufen, weil die ausdrücklichen Einwilligungen der Betroffenen vor den Fallkonferenzen eingeholt werden können. Diesen Einwilligungen müssten

allerdings einzelfallbezogene Informationen über den Zweck der Datenverarbeitung und über die an der Fallkonferenz beteiligten Behörden vorausgehen. Unter diesen Umständen ist fraglich, ob die Betroffenen in jedem Fall ihr Einverständnis erklärt hätten, zumal sie selbst an den Konferenzen nicht teilnehmen dürfen.

Kurz vor Ende des Berichtszeitraumes haben wir uns bei einem Besuch bei der Polizei über den praktischen Ablauf der bisher durchgeführten Fallkonferenzen informiert. Dabei haben wir einige Anregungen zum Verfahrensablauf gegeben, die sich sofort umsetzen lassen, ohne das bisherige Konzept grundlegend zu verändern. Dabei handelte es sich insbesondere um Hinweise zu den Speicherfristen, zur verschlüsselten Datenübermittlung, zur Vernichtung von Daten und zur Konzeption von Einwilligungserklärungen, die von den Betroffenen eingeholt werden sollen. Die Mehrzahl unserer Anregungen wurde bereits umgesetzt. Wir werden das Verfahren der behördenübergreifenden Fallkonferenzen weiter kritisch begleiten und dazu beitragen, dass die Praxis datenschutzgerecht ausgestaltet wird.

8. Bildung

8.1 Videoüberwachung in Schulen

Das Hamburgische Schulgesetz enthält jetzt eine Rechtsgrundlage für die Videoüberwachung in Schulen.

Zur Umsetzung der im Regierungsprogramm vorgesehenen Schulreform hat der Senat der Bürgerschaft Mitte 2009 den Entwurf eines Gesetzes zur Änderung des Hamburgischen Schulgesetzes (HmbSG) vorgelegt. Darin wurden im Wesentlichen umfassende Veränderungen im Aufbau und in den organisatorischen Rahmenbedingungen des hamburgischen Schulwesens festgeschrieben. Mit der Schulgesetznovelle blieb der Siebte Teil des Schulgesetzes, der den Datenschutz regelt, unangetastet. Dennoch hatten wir Veranlassung, uns mit dem Gesetzesvorhaben zu beschäftigen.

Wegen unserer wiederholt vorgetragenen Kritik an der fehlenden Ermächtigungsgrundlage für die Videoüberwachung in Schulen (vgl. 21. TB, 13.4) hatte sich der Senat entschieden, die Videoüberwachung im Schulgesetz zu verankern. Die Behörde für Schule und Berufsbildung (BSB) hat daraufhin eine entsprechende Regelung in § 31 Abs. 4 HmbSG erarbeitet, die uns mit einer sehr kurzen Frist zur Stellungnahme vorgelegt wurde. Wir haben uns dann auf folgende Regelung verständigt:

Die optisch-elektronische Überwachung von Schulräumen und schulischen Freiflächen (Videoüberwachung) und die Verarbeitung der dabei erhobenen Daten sind nur dann und so lange zulässig, wie sie zur Abwehr von konkreten Gefahren für die persönliche Sicherheit von Personen oder den Erhalt schulischer Einrichtungen oder in die Schule eingebrachter Sachen erforderlich und verhältnismäßig sind. Eine Überwachung des Inneren von Klassenräumen, Beratungs- und Lehrerzimmern, sanitären Anlagen und Umkleideräumen ist nicht zulässig. Über die Einrichtung entscheidet die zuständige Behörde auf Antrag der Schulleitung unter Einbeziehung der oder des behördlichen Datenschutzbeauftragten. Diesem Antrag sind eine Stellungnahme des schulischen Personalrats und eine Verfahrensbeschreibung und Risikoanalyse beizufügen. Die Erforderlichkeit solcher Maßnahmen ist nach Ablauf eines Jahres erneut zu bewerten. Überwachte Bereiche sind zu kennzeichnen. Der Senat wird ermächtigt, durch Rechtsverordnung nähere Regelungen über die Verarbeitung im Zuge der Videoüberwachung gewonnener Daten und zu den Auskunftspflichten

zu treffen. Die Verordnung regelt insbesondere Art und Umfang der zu verarbeitenden Daten, Dateiformate und technische Wege der Datenübermittlung, technische und organisatorische Maßnahmen und Maßnahmen zur Datenschutzkontrolle, Aufbewahrungsfristen sowie das Verfahren bei der Ausübung des Rechtes auf Auskunft und Einsicht in Unterlagen.

Die Bürgerschaft hat die Schulgesetznovelle mit dieser neuen Bestimmung am 7.Oktober 2009 verabschiedet. Bevor die Schulen auf dieser Grundlage mit der Installation von Videoüberwachungsanlagen beginnen dürfen, muss noch – wie vom Gesetzgeber verlangt – in einer Rechtsverordnung das Nähere geregelt werden. Bis zum Redaktionsschluss hat uns der Senat noch keinen entsprechenden Verordnungsentwurf zur Stellungnahme vorgelegt.

8.2 Regionale Beratungs- und Unterstützungsstellen (REBUS)

Sensible Daten werden in einer Datenbank verarbeitet, ohne dass klar ist, ob das Verfahren den datenschutzrechtlichen Anforderungen genügt.

Die Regionalen Unterstützungsstellen (REBUS) werden tätig, wenn schulische Probleme von Schülerinnen und Schülern nicht aus eigener Kraft der Beteiligten bewältigt werden können und diese sich an REBUS um Hilfe wenden. REBUS versteht die Beratungs- und Unterstützungsleistungen als Hilfe zur Selbsthilfe. Sie werden am Einzelfall mit den Beteiligten erarbeitet mit dem Ziel, gefährdete Schülerinnen und Schüler in ihrer schulischen Entwicklung zu stabilisieren bzw. in schulische Angebote zu reintegrieren. REBUS entwickelt ein Angebot von Hilfen abgestimmt auf die spezifischen regionalen Strukturen und die entsprechenden Unterstützungsbedarfe. Das Angebot setzt sich zusammen aus Diagnostik, Beratung und Unterstützung. Die Dienststellen sind multiprofessionell mit Schulpsychologen, Lehrkräften/Sonderpädagogen, Sozialpädagogen und Verwaltungskräften besetzt.

Es liegt auf der Hand, dass bei diesem Aufgabenspektrum sehr sensible Daten verarbeitet werden, die besonders zu schützen sind. Folglich verlangte §99 Abs. 3 Hamburgisches Schulgesetz (HmbSG) bis 2006, dass die im Schulberatungsdienst eingesetzten Datenverarbeitungsgeräte nicht mit Datenverarbeitungsgeräten, die für andere Aufgaben benutzt werden, vernetzt werden dürfen. Da sich die technischen Schutzmöglichkeiten auch in vernetzten Systemen weiter entwickelt haben, hat der Gesetzgeber das Vernetzungsverbot aufgehoben. Der neu gefasste §99 Abs. 3 HmbSG verlangt jedoch, dass Daten, die von den für den Schulberatungsdienst zuständigen Stellen – also REBUS – verarbeitet werden, sicher gegen Einsichtnahme und Verarbeitung anderer Stellen, auch der Schulen und der für das Schulwesen zuständigen Behörde, geschützt sein müssen. Die Umsetzung dieser gesetzlichen Anforderung erfordert vielfältige technische und organisatorische Maßnahmen.

Im März 2007 erhielten wir von der Behörde für Schule und Berufsbildung (BSB) sowohl die Verfahrensbeschreibung als auch die Risikoanalyse für eine neue Datenbank, mit der die Regionalen Beratungs- und Unterstützungsstellen (REBUS) in ihrer Tätigkeit unterstützt werden sollten. Die uns vorgelegten Papiere enthielten zu den erforderlichen Schutzmaßnahmen nur unzureichende Darstellungen, so dass wir die BSB auffordern mussten, entsprechend nachzubessern.

Ein halbes Jahr später erhielten wir eine veränderte Verfahrensbeschreibung, die nach wie vor nicht alle unsere Fragen zufriedenstellend beantwortete. Eine neue

Risikoanalyse wurde uns zunächst überhaupt nicht vorgelegt, sondern die BSB nahm sich dafür Zeit bis zum März 2009. Mit derselben Post erhielten wir eine nochmals überarbeitete Verfahrensbeschreibung. Umso überraschter waren wir, als wir lediglich beiläufig zum ersten Mal davon erfuhren, dass das Datenbankverfahren bereits seit Dezember 2007 produktiv an den REBUS-Standorten eingesetzt wird.

Leider sind trotz der überarbeiteten Unterlagen nach wie vor zahlreiche datenschutzrechtliche Fragen offen. Beispielsweise konnte uns die BSB bislang nicht erläutern, auf welcher Rechtsgrundlage die automatisierte Verarbeitung der personenbezogenen Daten bei REBUS überhaupt zulässig ist. Sowohl das Hamburgische Schulgesetz (HmbSG) als auch die Schul-Datenschutzverordnung enthalten jedenfalls keine entsprechenden Befugnisnormen. Die BSB hat uns nicht nachvollziehbar darstellen können, durch welche technischen und organisatorischen Maßnahmen die Daten im REBUS-Verfahren sicher gegen eine Einsichtnahme und Verarbeitung anderer Stellen, auch der Schulen und der BSB, geschützt sind, so wie dies § 99 Abs. 3 HmbSG zwingend vorschreibt.

Daneben gibt es noch weitere ungeklärte Fragen oder es wurden Hinweise, die wir gegeben haben, nicht umgesetzt. Deshalb bedarf es noch einiger Anstrengungen der BSB, das REBUS-Verfahren den datenschutzrechtlichen Anforderungen anzupassen. Wir hoffen aber, dass dies im Zuge der Neubesetzung der Stelle eines behördlichen Datenschutzbeauftragten zügig geschehen wird.

8.3 Zentrales Schülerregister

Unsere datenschutzrechtlichen Bedenken konnten bislang nicht vollständig ausgeräumt werden.

Das Zentrale Schülerregister (ZSR) ist vor fast 3 Jahren eingeführt worden. Von Beginn an gab es damit datenschutzrechtliche Probleme, auf die wir die Behörde für Schule und Berufsbildung (BSB) hingewiesen haben (vgl. 21 TB, 13.1). Leider gibt es immer noch einige Kritikpunkte:

- Die BSB hatte zur Einführung des ZSR eine Risikoanalyse nach § 8 Abs. 4 HmbDSG erstellt und uns zugeleitet. Zahlreiche Punkte darin waren aus datenschutzrechtlicher Sicht nicht zufriedenstellend dargestellt, so dass wir die BSB bitten mussten, die Risikoanalyse entsprechend zu überarbeiten. Erst kurz vor Redaktionsschluss hat uns die BSB eine neue Risikoanalyse vorgelegt, die den aktuellen Stand des ZSR-Verfahrens hinreichend widerspiegeln soll. Wir werden untersuchen, ob damit unsere Kritik an der bisherigen Risikoanalyse erledigt ist.
- Im Zusammenhang mit der Einführung des ZSR erfolgte eine Anpassung der Meldedatenübermittlungsverordnung. So werden auch die Anschriften von Schülerinnen und Schülern sowie ihrer Sorgeberechtigten, die einer melderechtlichen Auskunftssperre unterliegen, aus dem Melderegister an das ZSR übermittelt. Wir können bislang aber nicht erkennen, dass die BSB die erforderlichen Maßnahmen getroffen hat, um dem besonderen Schutzbedarf dieses Datums im ZSR Rechnung zu tragen. Dass dies erforderlich ist, macht folgendes Beispiel deutlich:

  Neben den staatlichen Schulen, die in das FHHNet eingebunden sind, wird den privaten Schulen der Zugang zum ZSR über das Internet (HamburgGateway) ermöglicht. Für diesen Zugang hatten wir zusätzliche Schutzmaßnahmen gefordert, wie z.B. den Einsatz von Signaturkarten. Die BSB kommt in ihrer Risikobetrachtung zu dem Schluss, dass nicht garantiert werden kann, dass der Zugriff

auf das ZSR tatsächlich aus einem geschützten Bereich heraus erfolgt. Zusätzliche Schutzmaßnahmen wurden bisher dennoch nicht getroffen.

- Es mangelt nach wie vor an einem schlüssigen Berechtigungskonzept. Unsere Kritik an den unzureichenden technischen und organisatorischen Maßnahmen, die wir in unserem 21. TB geäußert haben, gilt uneingeschränkt fort.

Die geschilderten Datenschutzprobleme haben uns veranlasst, in eine datenschutzrechtliche Prüfung des ZSR nach § 23 Abs. 1 HmbDSG einzusteigen. Bei Redaktionsschluss dauerte diese Prüfung zwar noch an. Die ersten Ergebnisse scheinen aber unsere Kritik am Betrieb des ZSR zu bestätigen. Mit Blick auf die künftige Zusammenarbeit hoffen wir, dass die offenen Punkte möglichst zügig beseitigt werden.

8.4 Zusammenarbeit mit der Behörde für Schule und Berufsbildung (BSB)

Zahlreiche Informationsdefizite in der Vergangenheit – positiver Trend für die Zukunft.

Leider haben wir in der Vergangenheit Informationen zur datenschutzrechtlichen Beurteilung oft zu spät erhalten. Im Rahmen unserer Beteiligung an verschiedenen IT-Vorhaben der BSB war es immer wieder erforderlich, die BSB um Beantwortung von Fragen zu bitten, um die Verfahren datenschutzrechtlich bewerten zu können. Eine Praxis, die in unserem Umgang mit den Behörden zum Alltag gehört. In aller Regel kam es dann zu Besprechungen, in denen versucht wurde, unsere Fragen zu klären. Wenn dies nicht gleich gelang, sagte man uns schriftliche Antworten zu. Hierzu ist die BSB nach § 23 Abs. 5 Hamburgisches Datenschutzgesetz (HmbDSG) auch verpflichtet, denn die öffentlichen Stellen haben uns bei der Erfüllung unserer Aufgaben zu unterstützen und uns dabei insbesondere die erbetenen Auskünfte zu erteilen. Dies beinhaltet natürlich auch eine Bearbeitung unserer Anfragen in einer angemessenen Zeit.

Im Berichtszeitraum sind unsere Anfragen von der BSB in zahlreichen Fällen nur sehr schleppend beantwortet worden. So dauerte es beispielsweise mehr als ein halbes Jahr, bis wir eine Antwort auf unsere Rückfragen zum Zentralen Schülerregister erhielten (vgl. III 8.3), und dies auch nur nach mehrfacher Erinnerung.

Unbefriedigend war auch, wie die BSB mit unseren Hinweisen zu neuen IT-Verfahren umgegangen ist. So haben wir die BSB zum Beispiel bereits im April 2007 auf zahlreiche datenschutzrechtliche Defizite bei einem Verfahren hingewiesen, mit dem personenbezogene Daten bei den Regionalen Beratungs- und Unterstützungsstellen (REBUS) verarbeitet werden. Bei REBUS handelt es sich um eine Dienststelle der BSB, die zahlreiche Aufgaben rund um die sonderpädagogische, sozialpädagogische und psychologische Beratung bei Leistungs- und Verhaltensproblemen von Schülern wahrnimmt. Entsprechend sensible Daten werden von REBUS verarbeitet. Unsere Hinweise wurden bis zum Redaktionsschluss nicht bzw. nur unzureichend aufgegriffen. Hinzu kommt, dass wir trotz regelmäßiger Sachstandsanfragen von der Produktivsetzung des Verfahrens im Dezember 2007 erst ca. 6 Monate später erfahren haben, und dies, obwohl zahlreiche datenschutzrechtliche Fragen weiter offen sind (vgl. III 8.2).

Die Situation besserte sich, nachdem die BSB im Sommer 2009 eine behördliche Datenschutzbeauftragte bestellte. Sie hat sofort Kontakt mit uns aufgenommen, um zu klären, welche Defizite noch abzuarbeiten waren. Das führte dazu, dass einige offene Punkte erledigt werden konnten. Diese Entwicklung begrüßen wir. Sie bestärkt unsere Auffassung, dass eine spürbare Verbesserung der Kooperation zwi-

schen den hamburgischen Behörden und uns ganz entscheidend von der Bestellung behördlicher Datenschutzbeauftragter abhängt. Daneben trug auch ein Wechsel in der Leitung des Referats IT-Management zu einer besseren Kommunikation zwischen uns und der BSB bei.

Leider hat die behördliche Datenschutzbeauftragte der BSB eine Aufgabe in einem anderen Bundesland übernommen und konnte die begonnene positive Entwicklung nicht weiterführen. Wir haben jedoch mit Erleichterung zur Kenntnis genommen, dass die BSB die Stelle bereits neu ausgeschrieben hat. Deshalb hoffen wir auf eine zügige Nachfolgeregelung und auf die Fortsetzung des positiven Trends der Zusammenarbeit.

8.5 Datenschutz in den Schulen

Einige Lehrkräfte müssen noch für den Datenschutz sensibilisiert werden.

Originäre Aufgabe der Lehrkräfte ist es, den gesetzlichen Bildungs- und Erziehungsauftrag der Schule zu erfüllen. Die hierbei anfallenden personenbezogenen Daten der Schülerinnen und Schüler dürfen aber nur im notwendigen Umfang erhoben, verarbeitet oder an andere Stellen übermittelt werden. Dies ist nicht der persönlichen Einschätzung der Lehrkräfte überlassen, sondern ergibt sich aus den Datenverarbeitungsnormen des Hamburgischen Schulgesetzes (HmbSG), das durch die Schul-Datenschutzverordnung sowie die allgemeinen Vorschriften des Hamburgischen Datenschutzgesetzes (HmbDSG) ergänzt wird. Den Lehrkräften sollte also diese Normendreifaltigkeit vertraut sein. Leider mussten wir feststellen, dass dies nicht immer der Fall ist, wie folgende Beispiele deutlich machen.

Eine Lehrkraft hatte die Ergebnisse einer Klausurarbeit in das Internet eingestellt, und zwar unter Angabe der vollständigen Schülernamen, der Schüler-Identifikationsnummern und Anmerkungen zu den erzielten Leistungen. Der Zugang zu diesen Daten war für jeden Internetnutzer weltweit möglich. Bei den veröffentlichten Daten handelte es sich um personenbezogene Daten im Sinne von § 4 Abs. 1 HmbDSG, die nicht offenkundig sind. Die Veröffentlichung dieser Daten im Internet ist rechtlich eine Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs, die nur unter den Voraussetzungen des § 16 HmbDSG zulässig gewesen wäre. Auf den vorliegenden Fall trafen jedoch keine der darin genannten Zulässigkeitsvoraussetzungen zu. Auch das Hamburgische Schulgesetz oder die Schul-Datenschutzverordnung lassen eine solche Veröffentlichung nicht zu. Die Veröffentlichung der Daten im Internet war mithin rechtswidrig.

In einem anderen Fall hatte eine Lehrkraft mehreren Schülerinnen und Schülern mitgeteilt, welche Note ein bestimmter anderer Schüler in einem Fach erhalten soll, obwohl sie den Schüler überhaupt nicht unterrichtet hatte. Der betroffene Schüler wurde daraufhin von seinen Mitschülern gemobbt. Wir konnten zwar nicht aufklären, wie die Lehrkraft von der Benotung des Schülers erfahren hatte und was sie bewogen hatte, ihr Wissen preiszugeben. Die Weitergabe einer Information aus dem Lehrerkollegium über einen einzelnen Schüler gegenüber Mitschülern – und sei es auch nur die Bestätigung eines Gerüchtes – ist aber datenschutzrechtlich nicht zulässig.

In beiden Fällen sind die Lehrkräfte von der Schulleitung dienstrechtlich gerügt worden. Unsere Prüfung, ob wir zusätzliche Maßnahmen gegen die Lehrkräfte einleiten, dauerte bis zum Redaktionsschluss noch an. Die Beispiele zeigen aber, dass die Vermittlung datenschutzrechtlicher Grundsätze bei den Lehrkräften noch

verbesserungswürdig ist. Besonders gefordert hierbei sind die Schulleitungen und die Behörde für Schule und Berufsbildung. Wir sind zuversichtlich, dass unser gemeinsam mit der BSB gestartetes Projekt „Meine Daten kriegt ihr nicht!" zur Förderung der Datenschutzkompetenz bei Schülerinnen und Schülern (s. unter I. 3.1.2) auch eine Stärkung des Datenschutzbewusstseins bei den Lehrkräften bewirken wird.

9. Gesundheitswesen

9.1 Elektronische Patientenakte im Krankenhaus

Auf die elektronische Patientenakte dürfen rechtlich nur Krankenhausmitarbeiterinnen und -mitarbeiter zugreifen, die tatsächlich mit der Behandlung des Patienten und ihrer verwaltungsmäßigen Abwicklung befasst sind. Technisch gehen die Zugriffsmöglichkeiten meist weit über diesen Personenkreis hinaus und gefährden damit den Patientendatenschutz.

Ein Missbrauchsfall im UKE hatte deutlich gemacht, dass insbesondere bei prominenten Patienten die Versuchung für Krankenhausmitarbeiter groß ist, auch ohne eigene Zuständigkeit sensible Informationen über eine erkrankte Person zu erlangen und gegebenenfalls auch weiterzugeben. Nach dem Hamburgischen Krankenhausgesetz (HmbKHG) ist dies jedoch auszuschließen: „Patientendaten sind so zu speichern, dass nur solche Mitarbeiterinnen und Mitarbeiter Kenntnis nehmen können, die die Patientendaten zur rechtmäßigen Erfüllung der ihnen obliegenden Aufgaben benötigen", §8 Abs.2 HmbKHG.

Die Logik der Krankenhausinformationssysteme, die die Zugriffsmöglichkeiten auf die elektronischen Patientenakten regeln, ist jedoch eine ganz andere: Nicht konkrete Krankenhausmitarbeiter erhalten ein Zugriffsrecht, sondern mehr oder weniger große Organisationseinheiten oder Mitarbeitergruppen. Damit wird verhindert, dass bei unvorhergesehener Abwesenheit der behandelnden und zugriffsberechtigten Personen die notwendigen Patientendaten für die Vertretung nicht mehr zur Verfügung stehen. In kleineren Häusern wird oft allen Ärzten und Ärztinnen, in mittleren Häusern zumindest allen Oberärzten der Zugriff auf die Daten aller Patienten des Krankenhause eingeräumt. In größeren Häusern erhalten alle Ärzte und Ärztinnen einer bestimmten Fachrichtung den Zugriff auf Daten aller Patienten, die dieser Fachrichtung zugeordnet wurden.

Medizinisches und Funktionspersonal, das mehreren Fachrichtungen angehört oder in zentralen Pools auf Anforderung für alle Patienten da ist – z.B. Anästhesisten, Physiologen, Sozialarbeiter -, erhält als Gruppe Zugriffsrechte auf sehr viele Patienten, die der einzelne Gruppenangehörige gar nicht kennenlernt und auch nicht mitbehandelt. Dasselbe gilt für das Pflegepersonal, wenn es fachrichtungs- und stationsübergreifend eingesetzt wird.

In der Regel ist der Kreis der Patienten, auf deren Daten ein Krankenhausmitarbeiter oder eine Krankenhausmitarbeiterin zugreifen kann, wesentlich größer als der Kreis von Patienten, auf deren Daten ein Krankenhausmitarbeiter wegen seiner Beteiligung an der Behandlung zugreifen darf.

Verschärft wird die datenschutzrechtliche Problematik dadurch, dass den Patienten bei der Aufnahme regelmäßig die Einwilligung abverlangt wird, dass „der behandelnde Arzt" – in Wahrheit: die ganze Organisationseinheit bzw. Fachrichtung – auch in alle früheren Behandlungsdaten des Patienten in demselben Krankenhaus

Einsicht nehmen darf. Damit erweitert sich neben dem Kreis der (technisch) Zugriffsberechtigten auch der Zugriffsumfang auf Daten, die für eine Behandlung nicht immer erforderlich sind. In vielen Fällen erscheinen Zweifel an der notwendigen Freiwilligkeit der abverlangten Einwilligung angebracht. Beschwerden beim Datenschutzbeauftragten zeigen, dass Patienten vor allem frühere Aufenthalte in der psychiatrischen oder psychosomatischen Abteilung des Krankenhauses nicht gerne unnötigerweise offenbaren.

Eine weitere Vertiefung erfährt das datenschutzrechtliche Risiko elektronischer Patientenakten durch unzureichende Sperrungs- und Löschungsmöglichkeiten. Die Dauer der technischen Zugriffsfähigkeit geht vielfach über das erforderliche Maß weit hinaus. Es soll damit sichergestellt werden, dass bei einer unvorhergesehenen Wiederaufnahme desselben Patienten – z.B. als Notfall – die notwendigen Behandlungsinformationen sofort verfügbar sind.

So nachvollziehbar und legitim die Ansprüche der Krankenhäuser an die Verfügbarkeit der Patientendaten auch sind – sie sind abzustimmen mit dem ebenso berechtigten Interesse von prominenten Patienten, von Krankenhausmitarbeiterinnen und -mitarbeitern, die sich in „ihrem" Krankenhaus behandeln lassen, von Nachbarn, Bekannten und Freunden des Krankenhauspersonals an der eigenen „informationellen Selbstbestimmung" und der Einhaltung der ärztlichen Schweigepflicht. Bei den Zugriffen auf Patientendaten muss die Lücke zwischen rechtlichem Dürfen und technischem Können, die durch moderne integrierte Krankenhausinformationssysteme eher größer als kleiner wird, so weit wie möglich wieder verkleinert bzw. geschlossen werden.

Wie dies zu bewerkstelligen ist, hängt einerseits von den jeweils eingesetzten Softwaresystemen, andererseits von der Größe und den medizinisch erforderlichen Organisationsstrukturen des einzelnen Krankenhauses ab. Vielfach müssen neben den Medizinern und Krankenhausleitungen auch die Hersteller der Systeme sensibilisiert und mit den Anforderungen des Datenschutzes vertraut gemacht werden.

Nach Prüfungen im Universitäts-Klinikum Eppendorf (UKE) und bei der Asklepios Hamburg GmbH sowie Erörterungen mit den Datenschutzbeauftragten der Hamburger Krankenhäuser machten wir im Juni 2009 die datenschutzrechtlichen Risiken von elektronischen Patientenakten in einer Pressekonferenz publik. Gleichzeitig veröffentlichten wir einen 40-Punkte-Katalog mit „Normativen Eckpunkten für Zugriffe auf elektronische Patientendaten im Krankenhaus". Die erfreuliche Medienreaktion bewirkte, dass dieses Thema sowohl mit den Hamburger Krankenhäusern als auch bundesweit in Fachkreisen und einer Arbeitgruppe der Datenschutzbeauftragten nun weiter diskutiert wird. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder griff das Thema in ihrer Herbst-Tagung 2009 auf und formulierte in einer Entschließung datenschutzrechtliche Anforderungen an Krankenhausinformationssysteme. In weiterführenden Gesprächen mit der Hamburgischen Krankenhausgesellschaft konnten wir hinsichtlich der Zielperspektive Übereinstimmung erreichen.

9.2 Prüfungen im Universitäts-Klinikum Eppendorf

Bei Prüfungen des Ambulanzzentrums, des neuen Klinischen Arbeitsplatzsystems SOARIAN und des Universitären Tumorzentrums UCCH stießen wir auf eine Reihe von Datenschutzmängeln. Zum Teil wurden sie inzwischen behoben, zum Teil werden sie zur Zeit im Dialog mit dem UKE abgearbeitet. Grundsätzliche datenschutzrechtliche Probleme bereitete die Ausdifferenzierung der „UKE-Gruppe" in rechtlich

selbstständige und unselbstständige Teil-Organisationen bei gleichzeitigem Anspruch, medizinisch eine Einheit mit integrierter Informations- und Kommunikationsstruktur zu bilden.

Das im Mai und Juni 2008 geprüfte Ambulanzzentrum des UKE ist eine rechtlich eigenständige GmbH. Mangels stationärer Patientenaufnahme gilt das Hamburgische Krankenhausgesetz mit seinen gesetzlichen Datenverarbeitungsberechtigungen nicht; mangels rechtlicher Zugehörigkeit zur öffentlich-rechtlichen Körperschaft UKE gilt auch das Hamburgische Datenschutzgesetz nicht, sondern nur das Bundesdatenschutzgesetz (BDSG) mit seinen Generalklauseln für den nichtöffentlichen Bereich. Diese Rechtsstellung des Ambulanzzentrums hat zur Folge, dass die Patientendatenverwaltung einschließlich der Archivierung der Behandlungsakten grundsätzlich nur Ambulanz-intern erfolgen darf. Übermittlungen von Patientendaten an UKE-Kliniken bedürfen ebenso einer gesonderten Einwilligung des Patienten wie der Zugriff auf Daten eines Ambulanzpatienten aus früheren Behandlungen in einer UKE-(Kern-)Klinik. Dasselbe gilt für die Auftragsdatenverarbeitung, die z.B. darin liegt, dass das Ambulanzzentrum die technische und personalwirtschaftliche UKE-Infrastruktur nutzt. Personalidentitäten zwischen UKE- und Ambulanz-Ärzten (jeweils Teilzeit-Beschäftigung oder Doppelfunktion) führen zu Schwierigkeiten etwa bei den Zugriffsberechtigungen.

Bei unserer Prüfung wurde offenbar, dass bei der Ausgründung von selbstständigen Tochterunternehmen kaum oder gar nicht an die datenschutzrechtlichen Konsequenzen gedacht wurde. Die Lösung über entsprechende Einwilligungen ist kein „Allheilmittel": Nach § 4 a BDSG muss eine Einwilligung auf der freien Entscheidung des Betroffenen beruhen, und sie ist jederzeit widerruflich. In vielen Fällen dürfte die Freiwilligkeit der Einwilligung zweifelhaft sein und die praktische Auswirkung einer abgelehnten, unwirksamen oder widerrufenen Einwilligung völlig unklar. (Nicht zuletzt aus diesem Grunde gilt im Sozialrecht eine strenge Gesetzesbindung, welche Einwilligungen als Ergänzung zu abschließend geregelten Datenverarbeitungen weitgehend ausschließt.)

Unsere Forderungen an das Ambulanzzentrum im Anschluss an die Prüfung richteten sich vor allem darauf, die datenschutzrechtlich notwendigen Konsequenzen aus der eigenen Rechtspersönlichkeit im Verhältnis zum Kern-UKE zu ziehen. Die grundsätzlichen Probleme der gesetzlich vorgesehenen Einwilligung konnten wir dabei nicht lösen (vgl. dazu 21. TB, 1).

Neben diesen strukturellen Datenschutzproblemen hatten wir Defizite bei der Administration des Datenverarbeitungssystems, bei der Aufbewahrung von Patientenakten einer zugekauften Arztpraxis und bei der Formulierung von Verfahrensbeschreibungen (SOPs) zu kritisieren.

Durch die zwischenzeitliche Übernahme des SOARIAN-Systems auch im Ambulanzzentrum wurde eine Reihe unserer Forderungen obsolet bzw. in die Prüfung dieses neuen Systems verlagert (s.u.). Im Übrigen trugen verschiedene Verbesserungen und Verfahrensänderungen unserer Kritik Rechnung. Mit einer erfolgreichen Nachschau im Juni 2009 konnten wir die Prüfung des Ambulanzzentrums abschließen.

Bei der 2008 begonnenen Prüfung des Universitären Cancer Center Hamburg (UCCH) – nun „Hubertus-Wald Tumorzentrum" – stellte sich das Problem der eigenen Rechtspersönlichkeit nicht. Das UCCH ist unselbständiger Teil des Kern-UKE. Es zeigten sich aber zwei andere Problemkomplexe:

Die stark interdisziplinäre Ausrichtung der „Tumorkonferenzen" ist medizinisch beispielhaft und für Studenten wie Assistenzärzte sehr lehrreich. Dies führt aber auch dazu, dass der Kreis der Personen, die die Gesundheitsdaten der in den Konferenzen vorgestellten Patienten zur Kenntnis nehmen, sehr groß ist. Hier vereinbarten wir mit dem UKE eine entsprechend aussagekräftige Aufklärung der Patienten, eine Einschränkung der Datenzugriffsberechtigung auf Fachärzte der teilnehmenden Fachrichtungen sowie die Möglichkeit einer pseudonymen Vorstellung externer Patienten durch den behandelnden Arzt. Offen sind noch Umfang und Dauer der Zugriffsberechtigungen aller an der Tumorkonferenz beteiligten Ärzte bzw. Fachrichtungen. Hier konkretisiert sich das strukturelle Datenschutzdefizit der elektronischen Patientenakte, s.u.

Der zweite Problemkomplex ist das Klinische Krebsregister des UCCH, das ursprünglich sowohl die Funktion der Behandlungsdokumentation als auch die Aufgabe einer Forschungsdatenbank erfüllen sollte. Das Hamburgische Krankenhausgesetz fordert jedoch eine klare Trennung zwischen Behandlungs- und Forschungsbereich. Wir machten deutlich, dass ein Klinisches Register zu Forschungszwecken nicht namensbezogen geführt werden darf, sondern allenfalls mit Pseudonymen, die nur die Behandelnden entschlüsseln können. Dies ist etwa erforderlich, wenn Daten aus anderen als UKE-Quellen in die Datenbank aufgenommen werden sollen. Über die genaue Ausgestaltung der Behandlungsdokumentation einerseits und des Klinischen Krebsregisters als Forschungsdatenbank andererseits sind wir mit dem UKE im Gespräch.

Besonders aufwändig gestaltete sich die Prüfung des neuen Klinik-Informationssystems SOARIAN, auch bezeichnet als KAS (Klinisches Arbeitsplatzsystem). Anlass war ein Missbrauchsfall, bei dem ein/e Krankenhausmitarbeiter/in auf Daten einer prominenten Patientin zugegriffen und Informationen an eine Zeitung weitergegeben hatte. Wir prüften jedoch nicht diesen Einzelfall, sondern die Sicherheit des Zugriffsberechtigungssystems insgesamt. Dazu werteten wir verschiedene Unterlagen aus, insbesondere das „Berechtigungskonzept für das Klinische Arbeitsplatzsystem (KAS)", und vollzogen in mehreren Treffen vor Ort die Zuordnung und technische Umsetzung der Zugriffsberechtigungen im System nach.

Unser Prüfbericht von Ende August 2009 machte deutlich, dass wesentlich mehr Krankenhausmitarbeiter/innen auf die elektronische Akte eines Patienten zugreifen können, als mit der Behandlung dieses Patienten befasst waren. Dies ergibt sich durch die Zuordnung des Patienten zu mehr oder weniger großen Abteilungen, den sog. Fachrichtungen. Alle in dieser Fachrichtung tätigen Mediziner können auf die Daten dieses Patienten zugreifen, unabhängig davon, ob der Arzt oder die Ärztin im Einzelfall an der Behandlung beteiligt ist. Gerade im UKE wird großer Wert auf die Interdisziplinarität der Behandlung gelegt – mit der Folge, dass viele Mediziner in mehreren Fachrichtungen tätig sind und die Daten der Patienten in allen seinen Arbeitsbereichen einsehen können, ohne dass es auf den Behandlungsbezug ankäme.

Bei Leistungs- oder Konsilanforderungen an andere Fachrichtungen, denen der Patient nicht zugeordnet ist, wird automatisch ebenfalls allen Mitgliedern dieser Fachrichtungen der Zugriff auf alle Daten dieses Patienten eingeräumt. Tatsächlich übernimmt meist aber nur eine Person die gewünschte Mitbehandlung. Dasselbe gilt für zentrale Einheiten und Funktionen wie Physiotherapeuten, Sozial- und Schreibdienste.

Da § 8 Abs.2 HmbKHG die Kenntnis der Patientendaten an die Erforderlichkeit zur konkreten Aufgabenerfüllung bindet, haben wir dem UKE aufgegeben, Vorschläge zur Eingrenzung der zu weit gehenden Zugriffsberechtigungen zu machen, und Hinweise dazu gegeben.

Unabhängig von der eigenen Fachrichtung wird darüber hinaus jedem Arzt, jeder Ärztin des UKE über den sog. „user contact" ein Not-Zugriff auf alle elektronischen Patientenakten eingeräumt – allerdings mit Warnhinweisen, Begründungsabfragen und einer Protokollierung. Wir baten hier um einen Erfahrungsbericht und ein Konzept zur Auswertung der Protokolle.

Weitere Kritikpunkte unseres Prüfberichts waren z.B. der Zugriff der Aufnahmekräfte auf die Abteilung früherer Behandlungen des aufzunehmenden Patienten, die Datenzugriffsorganisation nach Entlassung der Patienten, das Zusammenspiel der fachspezifischen Teilsysteme mit SOARIAN, die technische Umsetzung der Zugriffsrechteerteilung, die Passwortgestaltung, die Vergabe der Administrationsrechte sowie die Fernwartung.

In einer ersten Reaktion im Herbst 2009 stellte das UKE fest, dass es einzelne unserer Anregungen bereits umgesetzt habe, aber z.B. auf den „user contact" nicht verzichten könne. Hinsichtlich unserer anderen Forderungen, Prüfbitten und Vorschläge wird der Dialog fortgesetzt. Dabei gehen wir davon aus, dass die angestoßene bundesweite Diskussion um die Probleme der elektronischen Patientenakte (s.o. 9.1) auch für die Verbesserung von SOARIAN genutzt werden kann. Wir werden auf die Nutzung bestehender technischer Optionen zur Verbesserung des Datenschutzes drängen, uns aber auch darüber hinaus bemühen, im Kontakt zu Software-Herstellern diese Optionen zu erweitern.

9.3 Prüfung des Datenzugriffskonzepts in den Asklepios-Kliniken

Auch in den Kliniken der Asklepios Hamburg GmbH stellten wir Defizite bei der Zuordnung von Datenzugriffsberechtigungen fest. Im Rahmen der technischen Möglichkeiten wurden Verbesserungen erreicht und werden weitere angestrebt.

Im Anschluss an die Prüfung der Asklepios-Klinik Barmbek (21.TB 14.6) befassten wir uns mit dem „Ärztlichen Berechtigungskonzept SAP", das – mit Modifikationen in Details – in allen Asklepios-Kliniken eingesetzt wird. Ziel der Prüfung war es, technische Möglichkeiten herauszufinden, um die weiten Zugriffsrechte auf das vom Hamburgischen Krankenhausgesetz geforderte und medizinisch verantwortbare Maß zu reduzieren. Dabei ging es – ähnlich wie im UKE – um die Rollendefinitionen, über die das SAP-System die Berechtigung zum Zugriff auf Patientendaten steuert. Auch hier offenbarten sich die aus der Logik der elektronischen Patientenakte (s.o.) entstehenden Probleme: Statt der konkreten Aufgabe – wie gesetzlich gefordert -, folgt die Berechtigung zum Patientendatenzugriff der Zugehörigkeit zu einer bestimmten Organisationseinheit (Zentrum, Abteilung). Besonders weitgehende Rechte haben dabei z.B. Anästhesisten und Oberärzte.

Intensiv diskutiert wurde die Organisation der Zugriffsrechte bei Patienten, die nur kurzfristig in der Zentralen Notaufnahme ZNA behandelt werden. Dabei spielten die Einsatzorganisation für die ZNA, Konsilanforderungen an andere Fachabteilungen und die oft nur vorläufige Zuordnung des Patienten zu einer medizinischen Fachrichtung eine wesentliche Rolle.

In konstruktiver Kooperation mit dem betrieblichen Datenschutzbeauftragten der Asklepios Hamburg GmbH wurden verschiedene Varianten zur Eingrenzung der

Zugriffsrechte geprüft. Eine zunächst von der IT-Abteilung zugesagte Lösung verzögerte sich zunächst und wurde schließlich ganz verworfen. Es handelte sich um die von SAP im Anwenderhandbuch Klinisches System angebotene „Behandlungsbezogene Berechtigung", die mit dem sog. „temporären Behandlungsauftrag" zumindest das Problem des Datenzugriffs nach Entlassung des Patienten entschärft hätte. Der Probelauf zeigte jedoch erhebliche technische und organisatorische Konflikte, denen sich auch die datenschutzrechtlichen Anforderungen nicht verschließen konnten.

Im Mai 2009 wurden die „Sammelrollen" der Ärzte, die den Zugriffsberechtigungen zugrunde liegen, wesentlich vereinfacht und nur um einige „Add-on-Rollen" für bestimmte Funktionen wie Dokumentationsbeauftragte ergänzt. Am Widerstand der Ärzte wegen unzumutbaren Bedienungsaufwands scheiterte zunächst der Versuch, im Rahmen von Konsil-Anforderungen die bislang wenig datenschutzfreundlichen Zugriffe auf umfassende Patientenlisten aufzugeben. Ziel ist jedoch weiterhin, für jede Abteilung eine eigene Konsilanforderungseinheit zu schaffen, um die Zugriffsberechtigungen deutlich zielsicherer auf die tatsächlich angeforderte Leistung orientieren zu können. Insgesamt bleibt es aber bei der Rechtezuordnung an die Zugehörigkeit zu einer bestimmten Abteilung unabhängig von einer konkreten Behandlungsbeteiligung.

Die Auseinandersetzung mit der Asklepios Hamburg GmbH wird fortgeführt und orientiert sich unsererseits an dem oben (9.2) erwähnten Eckpunktepapier und der begonnenen Datenschutzdiskussion zur elektronischen Patientenakte. Die bisherigen Erfahrungen zeigen deutlich den prägenden Einfluss der technischen Systeme. Datenschutzrechtliche Anforderungen, die von diesen nicht sinnvoll umgesetzt werden können, sind in der Praxis kaum durchsetzbar. Aus unserer Sicht ist es daher entscheidend, dass die Hersteller von Krankenhausinformationssystemen Datenschutz von Anbeginn an in ihren Produkten verankern.

9.4 Neuregelung des Notdienstes der Kassenärztlichen Vereinigung

Auf unsere Kritik wurde der Vertrag zwischen der Kassenärztlichen Vereinigung Hamburg (KVH) und dem Dienstleister GARD zur Übernahme des ärztlichen Notdienstes modifiziert.

Erst durch die Zuschrift eines Bürgers erfuhren wir, dass die Neuorganisation des ärztlichen Notdienstes der KVH kurz bevorstand. Die angeforderten und im März 2008 zugesandten Ausschreibungsunterlagen machten deutlich, dass auf die Einhaltung des Datenschutzes bei der Reorganisation des ärztlichen Notdienstes zunächst nur geringe Aufmerksamkeit gerichtet war. Es war weder eine Risikoanalyse noch eine Verfahrensbeschreibung (§§ 8, 9 HmbDSG) vorgesehen. In einem konstruktiven Gespräch im April 2008 konnten dann mit der Projektleitung und dem internen Datenschutzbeauftragten die notwendigen Informationen ausgetauscht und folgende datenschutzrechtliche Verbesserungen vereinbart werden:

Ursprünglich war eine unbeschränkte Speicherung der Adress- und der Medizindaten der Notfall-Patienten sowohl auf dem Rechner der KVH als auch auf dem Rechner des Auftragnehmers GARD vorgesehen. Diese „Spiegelung" diente nicht zuletzt dem back up. Dies erschien angesichts der Sensibilität der Daten nicht vertretbar. Nun werden beide Datenarten auf dem KVH-Rechner nur noch 5 Jahre lang gespeichert – beschränkt auf Zwecke künftiger Einsätze, von Arzthaftungsprozessen und Rückfragen des Hausarztes zur Sachverhaltsaufklärung. Der privatrechtliche Auftragnehmer GARD darf nur die Kontakt-/Adressdaten der Patienten ebenfalls 5

Jahre speichern, um bei nicht voll kommunikationsfähigen (Notfall-)Patienten eine schnelle Adressermittlung zu ermöglichen. Die medizinischen Daten dürfen bei GARD nur noch 1 Jahr für spätere Rückfragen von behandelnden Ärzten oder Krankenkassen zur Verfügung stehen. Danach muss GARD die Daten löschen und auf die KVH verweisen. Diese Regelungen wurden im August 2008 in einer Ergänzungsvereinbarung zwischen der KVH und GARD fixiert.

Da es für die vorgesehene Patientendatenverarbeitung weder für die KVH noch für GARD eine spezialgesetzliche Grundlage gibt, bedurfte es einer Einwilligung des Patienten. Angesichts der Notfall-Situation und der ausschließlichen Datenverarbeitung im Interesse des Patienten haben wir uns ausnahmsweise zu einer Widerspruchlösung in möglichst einfacher Form bereiterklärt. In das Notfallprotokoll wurde der Satz aufgenommen: „Diese Patientendaten werden 5 Jahre gespeichert, wenn Sie dem nicht widersprechen." Ist der Patient ansprechbar, ist er darauf hinzuweisen. Auf eine ausdrückliche schriftliche Einwilligung haben wir „wegen besonderer Umstände" (§ 5 Abs.2 HmbDSG) verzichtet.

9.5 Früherkennungsuntersuchungen von Vorschulkindern

Die politischen Bemühungen, den Kinderschutz durch ein verbindliches Einladungsverfahren für die Früherkennungsuntersuchungen U 6 und U7 zu stärken, begleiteten wir von Anfang an und trugen – im Rahmen der Vorgaben – zu einer datenschutzgerechten Ausgestaltung bei.

Nachdem wir Initiativen und Konzepte zur Stärkung des Kinderschutzes aus anderen Bundesländern erhalten und diskutiert hatten, erreichten uns im Januar 2009 die ersten Anfragen und Konzepte der Behörde für Soziales und Gesundheit zu einem „verbindlichen Einladungswesen" zu den Früherkennungsuntersuchungen U6 und U7. Dabei ging es uns zunächst um eine klare Entscheidung zum Grad der Mitwirkungspflicht der Eltern und um die Schaffung erforderlicher Rechtsgrundlagen zur Datenverarbeitung, z.B. zur Übermittlung von Daten aus dem Melderegister oder an das Jugendamt.

Es folgte ein erster Gesetzentwurf zur Änderung des Gesundheitsdienstgesetzes. Das Konzept sah ein sehr komplexes Verfahren zwischen 6 beteiligten Stellen bzw. Personen mit einer außerhamburgischen Zentralstelle und einer Klärungsstelle bei einer Fachbehörde vor. In unserer Stellungnahme machten wir auf die notwendige Abgrenzung der Gesetzgebungskompetenzen zwischen Bund (Jugendschutzrecht) und Land (Gesundheitsrecht) aufmerksam, forderten eine Klärung der Elternpflichten und kritisierten eine geplante Rückmeldung von aktualisierten Adressdaten an das Melderegister ohne Kenntnis der Betroffenen.

Nach einem Gespräch mit der BSG erhielten wir im April einen überarbeiteten Entwurf, der die Neuregelungen nun als 2-jähriges Modellprojekt konzipierte. Im Juni folgte ein entsprechender Senatsdrucksachenentwurf mit Änderungsvorschlägen zum Gesundheitsdienstgesetz, zum Kinderbetreuungsgesetz und zur Meldedatenübermittlungsverordnung. Er berücksichtigte weitgehend unsere Anregungen. Von den wiederum neuen Regelungen kritisierten wir Bestimmungen zur Übermittlung des Todestages und der Staatsangehörigkeit.

Im September wurden die Entwürfe ein weiteres Mal verändert. Dies führte – neben der Berücksichtigung unserer Anmerkungen – einerseits zu einer klareren und konkreteren Beschreibung des vorgesehenen Verfahrens, enthielt aber andererseits neue Löschungsfristen und neue Informationswege nach einer endgültig nicht er-

folgten Früherkennungsuntersuchung: Nun soll die Zentrale Stelle die Personalien dieser Eltern und Kinder direkt an das Jugendamt weiterleiten, das aber nur prüft, ob es diesen Familien bereits Hilfe zur Erziehung leistet und in diesem Rahmen weitere Förderungsmaßnahmen ergreifen kann. In allen anderen Fällen reicht das Jugendamt die Daten der Familien an das zuständige Gesundheitsamt zur Wahrnehmung ihrer Aufgaben weiter. In unserer Stellungnahme forderten wir eine unmittelbare Datenlöschung in der Zentralen Stelle, wenn die Teilnahme an der Vorsorgeuntersuchung durch Eingang der Kinderarzt-Meldung festgestellt wurde, sowie im Übrigen eine Begrenzung der Speicherfrist auf 3 Monate. Ferner äußerten wir Bedenken gegen die unklare und unspezifische Datenverarbeitungsregelung für das Gesundheitsamt und im Rahmen des Kinderbetreuungsgesetzes.

Die vom Senat im Oktober beschlossene Gesetzesfassung trug unserem Anliegen einer möglichst frühzeitigen Datenlöschung ebenso Rechnung wie unserer Anregung, die konkreten Konsequenzen für die Gesundheitsämter zu benennen. Es bleibt das eher verfassungsrechtliche Problem, ob ein Landesgesetz den Jugendämtern außerhalb des Sozialgesetzbuchs VIII und X konkrete Aufgaben übertragen und Datenübermittlungen erlauben kann. Auch wirft die praktische Umsetzung der geplanten, aber nicht im Gesetz geregelten Evaluation des Verfahrens und der nur in der Gesetzesbegründung erwähnten „Abstimmung" zwischen Gesundheits- und Jugendamt datenschutzrechtliche Fragen auf. Wir baten darum, uns an deren Lösung zu beteiligen.

An dem parlamentarischen Experten-Anhörungsverfahren im November 2009 nahmen wir ebenso teil wie an der Senatsbefragung des zuständigen Bürgerschaftsausschusses. Diskussionspunkte waren unter anderem die Schweigepflicht der Kinderärzte und die rechtlichen Möglichkeiten zu einer Information des Jugendamtes zur Abwendung von Gefahren für das Kindeswohl – gegebenenfalls auch gegen den Elternwillen.

10. Forschung

10.1 Projekt LUCAS

Bei 5 Teilprojekten eines Großvorhabens der Altersforschung konnten wir im Dialog mit den verschiedenen Trägern datenschutzrechtliche Verbesserungen in der Organisation und der Probandenansprache erreichen.

Das Großprojekt LUCAS („Longitudinal Urban Cohort Ageing Study") erforscht in 7 Teilprojekten unterschiedliche Aspekte der Gesundheit im Alter. Träger sind das Albertinen-Krankenhaus, die Behörde für Soziales und Gesundheit, das UKE, die Hamburger Pflegegesellschaft und die Hochschule für Angewandte Wissenschaften. Bis auf das Albertinen-Krankenhaus erbaten diese Projektverantwortlichen unsere Beratung.

Zu Fragestellungen wie den folgenden konnten wir mit den Trägern jeweils datenschutzgerechte Lösungen finden:

- Wie musste die Rekrutierung der Probanden organisiert werden, die bereits an Vorstudien teilgenommen hatten; wie konnte das Melderegister genutzt werden?
- Wie musste die Information und Aufklärung der Probanden aussehen, um einerseits eine ausreichende Kenntnis der Probanden von der Datenverarbeitung zu

gewährleisten und andererseits eine Überforderung der betagten Betroffenen zu vermeiden ?

- Wie war die Einwilligungserklärung zu formulieren ?
- Wie mussten Telefon-Interviews vorbereitet und dokumentiert werden ?
- Wie war der Rücklauf von Fragebögen zu organisieren, um weitgehende Anonymität der inhaltlichen Angaben zu sichern und doch die Ablaufkontrolle und Zusammenführbarkeit der Daten zu wahren ?
- Welche Anforderungen mussten an die ergänzende Beschaffung von klinischen Daten oder Daten aus Pflegeheimen gestellt werden ?
- Wie war die Pseudonymisierung der Probandendaten für eine weitere Nutzung sicher zu gestalten ?

Es zeigte sich, dass bei frühzeitiger Einbeziehung des Datenschutzes auch sehr sensible Bereiche wie die psychische Situation von Vertriebenen im Alter, die Nutzung von „Biografiearbeit" bei der Betreuung im Pflegeheim und der Umgang mit Sturzgefahren und Gebrechlichkeit erforscht werden können, ohne den Respekt vor dem Selbstbestimmungsrecht und der Würde der Betroffenen aufzugeben.

10.2 Kleinräumige Gesundheitsberichterstattung Eimsbüttel

Bei diesem Projekt spielte vor allem die Anonymität der Einwohnerdaten bei einer Zuordnung von Einzeldatensätzen zu sog. statistischen Gebieten eine Rolle.

Das Gesundheitsamt Hamburg-Eimsbüttel plante 2008, seine Gesundheitsberichterstattung den politischen Ansprüchen an eine sozialräumliche Betrachtungsweise anzupassen. Dazu sollten verschiedene Einwohnerdaten für einzelne Quartiere wie die Lenzsiedlung und Schnelsen-Süd erhoben werden. Während die Statistikämter nach dem Bundesstatistikgesetz herkömmlich nur Daten zu Gemeinden (oder Stadt- bzw. Ortsteilen) oder zu Blockseiten zur Verfügung stellen, sollten nun Aussagen zu Gebieten getroffen werden, die zwischen diesen beiden Größeneinheiten liegen und hinsichtlich der sozialen Schichtung und der urbanen Verdichtung relativ homogen sind. Dafür wurden in Hamburg ab 1990 die sog. statistischen Gebiete gebildet.

Zu drei solchen statistischen Gebieten sowie zu 2 weiteren Gebiets-Gruppen sollten die Daten aus den Schuleingangsuntersuchungen, aus den schulzahnärztlichen Untersuchungen, aus dem Hamburger Krebsregister und aus den Geburts- und Todesursachenstatistiken ausgewertet werden.

Für die ersten beiden Quellen vereinbarten wir mit dem Bezirksamt, dass die Forscher keine personenbeziehbaren Daten aus den Schul(zahn)arztstellen mitnehmen durften, sondern sie vor Ort strukturiert erheben und aggregieren, also nur anonyme Daten weiter verarbeiten. So konnten die Anforderungen der Forschungsklausel im Hamburgischen Gesundheitsdienstgesetz erfüllt werden.

Auswertungen aus dem Hamburgischen Krebsregister konnten nach dem Krebsregistergesetz ebenfalls durch die Übermittlung aggregierter Daten erfolgen.

Probleme machte die Nutzung der Geburts- und Todesursachenstatistik, weil das Statistikamt Nord sich angesichts der Regelungen im Bundesstatistikgesetz gehindert sah, die Einzeldaten auf die gewünschten statistischen Gebiete zu beziehen. Aus datenschutzrechtlicher Sicht hatten wir dagegen weniger Probleme, wenn – unabhängig von der räumlichen Bezugsgröße – die Angabe von Einzeldaten ver-

mieden wurde, also von einer Anonymisierung der Daten ausgegangen werden konnte.

Mit einem „Vertrag zur Nutzung faktisch anonymisierter Daten" zwischen dem am Forschungsprojekt beteiligten Institut für Medizin-Soziologie des UKE und dem Statistikamt Nord wurde die gewünschte Datenübermittlung für das Forschungsprojekt dann möglich gemacht. Allerdings waren die vereinbarten Angaben zu „vermeidbaren Todesfällen" so differenziert, dass angesichts des kleinräumigen Bezuges viele Einzelangaben (Daten nur einer Person) wahrscheinlich waren. Wir baten deswegen um Prüfung, ob der Zweck der Forschung auch bei einer durchgehenden Aggregierung von Einzelangaben auf mehr als 2 Treffer erreicht werden kann. Die Strukturierung der vom Statistikamt zu übermittelnden Daten stellte allerdings sicher, dass Einzelangaben zu einem Merkmal keinen Schluss auf weitere Merkmale zu demselben Fall zuließen. Angesichts der im Vertrag festgelegten strengen Geheimhaltungspflichten und strafbewehrten Reidentifizierungsverbote haben wir deswegen unsere verbliebenen Bedenken auch für den Fall zurückgestellt, dass der Forschungszweck einer kleinräumigen Gesundheitsberichterstattung nur ohne eine durchgehende Aggregierung erreicht werden kann, die Ausweisung von Informationen zu nur einer (unbekannten) Person also in Kauf genommen werden müsste.

10.3 Veröffentlichung von Gruppenfotos

Die Veröffentlichung von Gruppenfotos im Rahmen eines privaten zeitgeschichtlichen Forschungsprojekts zu jeweils einem der Gruppenmitglieder begegnet datenschutzrechtlichen Bedenken.

Ein Polizeibeamter aus Berlin erforschte privat die näheren Umstände von im Dienst getöteten Polizisten und plante dazu eine Buchveröffentlichung. Darin sollten Gruppenfotos von den Getöteten zusammen mit ihren Dienstkollegen das soziale Umfeld der Opfer illustrieren. Die Fotos zeigten die – erkennbaren – Kollegen des Getöteten auch in dienstlicher bzw. dienstnaher Tätigkeit unter anderem als Volkspolizisten vor ihrem Einsatzfahrzeug, als Fußballspieler einer Betriebsmannschaft, als Musiker einer Polizeikapelle. Die Fotoaufnahmen lagen zwischen zehn und neunundzwanzig Jahren zurück. Einwilligungen der abgebildeten Kollegen in die Veröffentlichung der privaten Fotos lagen nicht vor.

Da es hier nicht um die Offenbarung personenbezogener Daten durch eine öffentliche (Polizeidienst-)Stelle, sondern um ein privates Forschungsprojekt ging, waren die Regelungen des Bundesdatenschutzgesetzes (BDSG) und des Kunsturhebergesetzes heranzuziehen. In unserer Stellungnahme machten wir aus zwei Gründen Einwände gegen das geplante Projekt geltend:

Die Forschungsklausel des BDSG stellt auf das „Interesse einer Forschungseinrichtung" und auf die Erforderlichkeit der Datenverarbeitung für die Durchführung des Forschungsvorhabens ab. Privatforschung, die keine wissenschaftlichen Ansprüche erfüllt, wird davon nicht erfasst. Dass die identifizierbare Darstellung der Kollegen für die Erreichung des Forschungszwecks unumgänglich war, wurde nicht begründet.

Nach dem Kunsturhebergesetz dürfen Bildnisse von „Personen der Zeitgeschichte" verbreitet werden. Dies gilt hier jedoch nur für die getöteten Polizisten selbst, nicht für deren Kollegen. Diese können andererseits auch nicht als zulässiges „Beiwerk" von Landschaftsbildern oder ähnlichem betrachtet werden. Sollen

sie einerseits für die Erfüllung des Forschungszwecks nach dem BDSG „erforderlich" sein, können sie andererseits nicht ein derart untergeordnetes Beiwerk darstellen, dass es „auch entfallen könnte, ohne dass Inhalt und Charakter des Bildes sich verändert" (Oberlandesgericht Oldenburg). Schließlich führt auch die erforderliche Abwägung zwischen dem Forschungs- und dem Betroffeneninteresse zu demselben Ergebnis: Gerade bei alten, vor der Grenzöffnung aufgenommenen Fotos berührt die Offenbarung einer früheren Zugehörigkeit zur damaligen Volkspolizei möglicherweise durchaus erhebliche (subjektive) Interessen der Abgebildeten.

11. Hochschulwesen

11.1 Projekt Hochschulübergreifendes Identitätsmanagement eCampus-IDMS

Sollen für ein hochschulübergreifendes Identitätsmanagement (IDMS) personenbezogene Daten aller Studierenden und aller Mitarbeiter von allen staatlichen Hochschulen Hamburgs zusammengeführt werden, so bedarf es hierfür einer rechtlichen Grundlage im Hamburgischen Hochschulgesetz (HmbHG). Die Daten sind auf das für die Aufgabenerfüllung erforderliche Maß zu beschränken. Trotz der geringen Sensibilität der einzelnen Daten sind angesichts der darüber erreichbaren Anwendungen Vorkehrungen für hohen bis sehr hohen Schutzbedarf zu treffen.

Vor dem Hintergrund des sog. Bologna-Prozesses, der ab 1999 eine einheitliche europäische Hochschullandschaft bis zum Jahre 2010 verwirklichen sollte, wuchs der Bedarf auch an hochschulübergreifender Datenverarbeitung. Dies stellte hohe Erwartungen und Anforderungen an die technische Infrastruktur.

Bereits im Herbst 2004 stellte uns die Multimedia Kontor Hamburg GmbH (MMKH), Gründung der staatlichen Hochschulen, erste Überlegungen für ein hochschulübergreifendes, hamburgweites Identitätsmanagement vor. Nach ersten Hinweisen unsererseits wollte man einen kaskadierenden Ansatz verfolgen, bei dem jede Hochschule Herrin über ihre Daten bleiben sollte und nur die erforderlichen Daten im Rahmen eines Meta Directory für eine konsolidierte, ständig aktuelle Datenbasis zur Aufbereitung von Authentifizierungs- und Autorisierungsverfahren einschließlich eines E-Mail-Accounts vorgehalten werden sollten.

Das bedeutet praktisch, dass jedes Hochschulmitglied hamburgweit nur eine Kennung erhält, über die es, je nach Zugriffsberechtigung, im Einzelfall Zugriff auf alle erdenklichen Verfahren an allen beteiligten Hochschulen erhält. Aus Komfortgründen war eine nur einmalige Anmeldung (single sign on) vorgesehen. Das Verfahren sollte neben den Hochschulmitgliedern auch Ehemalige beinhalten und über hochschuleigene Anwendungen hinaus das Deutsche Forschungsnetz sowie sonstige Kontakte zu dritten Stellen bedienen.

Die allgemeinen Vorteile von IDMS, wie Vermeidung von Redundanzen und Inkompatibilitäten, zentrales Berechtigungsmanagement sowie die verbesserte Einhaltung von Löschroutinen wurden auch hier betont.

Parallel dazu wurden vereinzelt zunächst hochschuleigene IDMS entwickelt.

Erst im Sommer 2008 wurde uns ein erster Entwurf einer Verfahrensbeschreibung übersandt. Kurzfristige Überlegungen, den gesamten Datenbestand aller Quellsysteme aller Hochschulen zusammenzuführen, wurden zurückgestellt. Entsprechend dem kaskadierenden Ansatz soll nun ein Katalog von 49 Daten zusammen-

geführt werden, um neben den Zugangsberechtigungen der einzelnen Hochschulen auch den Bibliothekenverbund der Hochschulen managen zu können.

Von der Einbindung des Deutschen Forschungsnetzes und weiterer außenstehender Stellen wurde abgesehen.

Ohne die Sinnhaftigkeit von IDMS an sich infrage zu stellen, war datenschutzrechtlich von zentraler Bedeutung zunächst die Frage nach einer hinreichenden Rechtsgrundlage zur Errichtung der übergeordneten, hochschulübergreifenden Datei.

Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn sie zur Aufgabenerfüllung erforderlich sind oder eine spezielle Vorschrift über den Datenschutz dies erlaubt. Die dritte Möglichkeit einer Einwilligungslösung schied von vornherein aus, da bei der unabdingbaren Möglichkeit eines jederzeitigen Widerrufs der Einwilligungserklärung das Verfahren unpraktikabel würde.

Das HmbHG regelt ausdrücklich bisher lediglich die Datenverarbeitungsbefugnis der eigenen Hochschule gegenüber ihren Mitgliedern und würde somit nur die Einrichtung eines hochschuleigenen IDMS zulassen.

Die allgemeinen Verarbeitungsvorschriften des HmbDSG setzen voraus, dass die Erforderlichkeit zum Zeitpunkt der Verarbeitung besteht und kein milderes Mittel zur Verfügung steht.

Danach könnte das hochschulübergreifende IDMS nur mit bereits bestehenden Aufgaben begründet werden und nur mit den dafür jeweils erforderlichen Daten.

Tatsächlich ist die hochschulübergreifende Zusammenarbeit bisher nur in einem einzigen Studiengang, nämlich „Gewerbelehramt" erforderlich. Ebenso ist es im Falle des Bibliothekenverbundes: nur die dafür erforderlichen Daten dürfen, wie in einem gesonderten automatisierten Verfahren bereits geschehen, gemeinsam verarbeitet werden.

Mit der Behörde für Wissenschaft und Forschung haben wir daher Einvernehmen erzielt, dass eine Regelung in das HmbHG aufgenommen werden soll. Dabei wird darauf zu achten sein, dass ein Verfahren gefunden wird, das der Bandbreite denkbarer hochschulübergreifender Vorhaben und ihrer Sensibilität jeweils angemessen Rechnung tragen kann.

Datenschutztechnisch ist zu berücksichtigen, dass über eCampus-IDMS letztlich alle automatisierten Verfahren der Hochschulen und der Staats- und Universitätsbibliothek erreicht werden können, mithin die sensibelsten und geheimsten Anwendungen. Dies wird nicht nur bei der Ausgestaltung des Verfahrens selbst, sondern zum Beispiel auch bei den Anforderungen zur Systemanmeldung und insbesondere in den Fällen, in denen das Passwort vergessen oder verloren wurde, zu berücksichtigen sein.

11.2 Chipkartenprojekte an Hochschulen

Sollen Studierendenausweise mit unterschiedlichen Funktionen oder sonstige Leistungen, die semesterübergreifend verwaltet werden müssen, per Chipkarte angeboten werden, sind hierfür hinreichend verbindliche Regelungen geboten. Die Hochschulen als verantwortliche Daten verarbeitende Stellen sollten hierfür eigene Karten ausgeben.

Im Berichtszeitraum wurden uns zwei Chipkartenprojekte vorgestellt:

Die Hochschule für angewandte Wissenschaften (HAW) hat uns erstmals im Jahre 2006 über das Vorhaben informiert, einen elektronischen Studierendenausweis mit Zusatzfunktionen einzuführen. Dies konkretisierte sich im Jahre 2008. Geplant waren Studierenden- und Bibliotheksausweis, Semesterticket, elektronische Zugangsberechtigung, Zahlfunktionen für Leistungen des Studierendenwerkes sowie Internationaler Studierendenausweis. Hierfür wurde im März 2008 eine Änderung der Immatrikulationsordnung vorgenommen, die im Wesentlichen die Rechtsverhältnisse an der Karte klärte, die Mitwirkungsrechte der Betroffenen und mögliche Einsatzbereiche der Karte beschrieb.

Zusätzlich wurde eine Regelung mit dem AStA angestrebt, wonach die Nutzung bis auf die Bereiche Studierendenausweis, elektronische Zutrittskontrolle und Semesterticket freiwillig sein sollte.

Wir haben angeregt, die Datenschutzsatzung der HAW als spezielle Rechtsgrundlage um die erforderlichen Daten und Funktionen zu ergänzen. Die Administration von freiwilligen Leistungen innerhalb eines Massenverfahrens ist vorab aufwändig durch die erforderliche Einholung der schriftlichen Einwilligung und nachträglich fehleranfällig durch die Administration von Widerrufen. Die Vereinbarung mit dem AStA hat datenschutzrechtlich keine konstitutive Wirkung. Übermittlungen von personenbezogenen Daten an den privaten Betreiber des Internationalen Studierendenausweises können erst bei bestehender Rechtsbeziehung erfolgen; deshalb waren Verfahren zu wählen, wonach zunächst nur eine für den Betreiber nicht zuordnungsfähige Ordnungszahl übermittelt wird, die für ihn erst durch die erste Nutzung zum Berechtigten zuordnungsfähig wird.

Datenschutztechnisch war sicherzustellen, dass eine hinreichend sichere Chiptechnik verwendet wird, dass der erforderliche E-Mail-Verkehr nur verschlüsselt erfolgt und dass das Verfahren bei Kartenverlust manipulationssicher gestaltet wird.

Ebenfalls im Jahre 2008 strebte die HafenCity Universität (HCU) die Einführung einer Studierendenkarte an, mit der ein Verfahren unterstützt werden sollte, in dem an die Studierenden Teile ihrer Semestergebühren zurückfließen sollten.

Angedacht war, die Studierenden möglichst unter Nutzung vorhandener Kreditkarten im Wege der Einwilligungslösung pro gebührenpflichtigem Semester eine bestimmte Punktzahl gutzuschreiben, die an autorisierten Stellen zur Zahlung von Dienstleistungen, Studienmaterialien und Zuschüssen eingelöst werden konnten. Das Punkteguthaben sollte semesterweise übertragbar sein und die abgefragten Leistungen sollten statistisch auswertbar sein um sicherzustellen, dass ein für alle Studiengänge attraktives Angebot vorgehalten wird.

Um aus den Eigentumsverhältnissen resultierende datenschutzrechtliche Probleme zu umgehen, haben wir empfohlen, ausschließlich mit hochschuleigenen Karten zu arbeiten, wie dies bereits an der Universität Hamburg und der HAW praktiziert wird.

Auch hier haben wir eine Ergänzung der Datenschutzsatzung empfohlen, um den Verwaltungsaufwand überschaubar zu halten.

Da die Regelung nicht rechtzeitig vor Einführung der Karte verabschiedet werden konnte, wurde übergangsweise mit der Einwilligung der Betroffenen gearbeitet.

In der Zwischenzeit konnten wir uns vom technischen Ablauf des Verfahrens ein Bild machen. Die Beantragung und buchhalterische Betreuung erfolgte anfangs noch in Papierform, für die Datenverarbeitung auf der Chipkarte wird eine Software aus dem Sparkassen-Umfeld in Anspruch genommen. Entsprechend hoch sind die technisch-organisatorischen Maßnahmen zur Datensicherheit ausgestaltet.

12. Geodaten

Geodateninfrastrukturgesetz

Unsere Beratung stellte eine datenschutzfreundliche Ausgestaltung der Bereitstellung und Nutzung von Geodaten im Gesetzentwurf sicher.

Im Juli 2008 beteiligten wir uns an der bundesweiten Diskussion zum Geodatenzugangsgesetz des Bundes und wirkten an einer Entschließung der Datenschutzkonferenz zu diesem Thema mit. Parallel dazu hatten wir uns mit dem Zugang zu den Geodaten des Kampfmittelräumdienstes (jetzt: Gefahrenerhebung Kampfmittelverdacht der Feuerwehr) zu befassen. Dabei ging es um die – für die Grundstückseigentümer durchaus wichtige – Frage: Wer darf in welchem Umfang über Bombenblindgänger- und Munitionsverdachtsflächen Auskunft erhalten? Dazu berieten wir sowohl den Landesbetrieb Geoinformationen und Vermessung (LGV) als auch die Feuerwehr: Das Hamburgische Vermessungsgesetz (HmbVermG) bezieht auch flächenbezogene Fachinformationsdienste in das Liegenschaftskataster ein. Die digitale Kartierung von Kampfmittelverdachtsflächen mit Auskunftserteilung ist als ein solcher Fachinformationsdienst anzusehen. Damit gelten die weitgefassten Rechte von Behörden und Versorgungseinrichtungen zu Zugriffen auf das Liegenschaftskataster auch für die Geodaten über Verdachtsflächen. Beschränkt sind dagegen die Informationsrechte von Privaten, die nicht Eigentümer des betroffenen Grundstücks sind.

Im Januar 2009 legte uns die Behörde für Stadtentwicklung und Umwelt einen ersten Entwurf für ein Hamburger Geodateninfrastrukturgesetz (HmbGDIG) vor. Es soll die europäische „INSPIRE-Richtlinie" (2007/2/EG) zur Förderung der Grundlagen für eine verstärkte Geodatennutzung umsetzen. Hauptdiskussionspunkt wurde das Spannungsverhältnis zwischen diesem Richtlinienziel und dem Schutz der betroffenen Grundstücksbesitzer und -eigentümer vor einer Verarbeitung und Veröffentlichung von personenbeziehbaren Geodaten. Dabei machten wir auf die keineswegs triviale Vorfrage aufmerksam, wann ein Geodatum überhaupt als ein personenbezogenes Datum anzusehen ist. Das Gesetz löst diese Frage nicht, sondern überlässt dies der Gesetzesanwendung im Einzelfall.

Wir trugen dazu bei, das Verhältnis zwischen dem GDIG, dem Hamburgischem Datenschutzgesetz und den bereichsspezifischen Datenschutzvorschriften zu klären. Der endgültige Gesetzentwurf räumt nun dem Datenschutz eindeutig Vorrang ein, soweit nicht der Zugang zu Informationen über Emissionen in die Umwelt betroffen ist. Dieser Vorrang gilt nun ausdrücklich auch für spezielle Datenschutznormen, wie sie z.B. im Krebsregistergesetz festgelegt sind. Dagegen soll parallel zum HmbGDIG auch das HmbVermG geändert werden mit dem Ziel, im Überschneidungsbereich beider Gesetze den Regelungen des HmbGDIG Vorrang einzuräumen. Auf diese Weise setzt sich z.B. auch hier der freie Zugang zu Umwelt-Emissionsdaten gegenüber dem Erfordernis eines berechtigten Interesses privater Dritter an der Kenntnis von Daten des Liegenschaftskatasters durch. Welche Folgen diese komplizierten Geltungsregelungen in der Praxis tatsächlich haben werden, ist aus

unserer Sicht noch offen. Ist etwa der Kampfmittelverdacht als Emission in die Umwelt zu bewerten – mit der Konsequenz, dass Datenschutz hier zukünftig generell zurücktritt? Wir gehen davon aus, dass die Nutzung der neuen Geodateninfrastruktur zur Bereitstellung, Verarbeitung und Veröffentlichung von Geodaten mit (potenziellem) Personenbezug im Einzelnen mit uns erörtert und abgestimmt wird.

13. Wahlen und Volksabstimmungen

13.1 Vordrucke für Briefwahlanträge im Postkartenformat

Im Berichtszeitraum wurde in Hamburg dreimal gewählt. Bei allen Wahlen kam es zu Nachfragen über die vorgefertigten Vordrucke zur Beantragung von Briefwahlunterlagen. Die Wahlbenachrichtigungen waren jeweils mit Antragsvordrucken im Postkartenformat versehen. Stein des Anstoßes war jeweils, dass damit für jedermann frei einsehbar Name, Geburtsdatum, vollständige Anschrift und Unterschrift sowie freiwillig auch Kontaktdaten übersandt werden sollten. Im Anschreiben zur Bürgerschaftswahl wurde ergänzend auf verschiedene sonstige Möglichkeiten zur Antragstellung hingewiesen.

§ 15 der Wahlordnung für die Wahlen zur Hamburgischen Bürgerschaft und zu den Bezirksversammlungen (HmbWO) enthält keine näheren Anforderungen an die Art des Postversands. Die angebotene Form genügte damit den wahlrechtlichen Bestimmungen. Auch ist der datenschutzrechtliche Verantwortungsbereich der Verwaltung erst mit Eingang des Antrags erreicht. Gleichwohl sollte dies nicht dazu führen, dass die Bürger durch staatliche Unterstützung dazu verleitet werden, die erforderlichen Daten ungeschützt zu übersenden. Wir baten das Landeswahlamt deshalb um Prüfung, ob der Antrag künftig wie in anderen Bundesländern auch ohne Adressfeld gedruckt werden könne, so dass dadurch eine datenschutzgerechte Übersendung des Antrags als Brief sichergestellt wird.

Aus Anlass der Europawahl enthielt der Vordruck den Hinweis: "Aus datenschutzrechtlichen Gründen wird die Übersendung in einem verschlossenen Briefumschlag (bitte ausreichend frankieren) empfohlen."

Wie mehrere Nachfragen dazu nahelegten, wurde dieser Satz offenbar leicht überlesen.

Zur Bundestagswahl wurde schließlich ein Kartenvordruck verwendet, in dem der zusätzliche Hinweis wieder verschwunden war. Stattdessen stand im Anschreiben an etwas versteckter Stelle: „Falls Sie Ihre Daten vor neugierigen Blicken schützen wollen, benutzen Sie bitte einen frankierten Briefumschlag."

Dieser Sachverhalt war nochmals anders zu bewerten:

Mit Anlage 4 zu § 19 Bundeswahlordnung sind Form und Inhalt des Antragsformulars bindend geregelt worden. Der Antrag ist als doppelseitiges DIN A4-Format vorgeschrieben und enthält auf der Rückseite den Hinweis: „Wahlscheinantrag ...bei Postversand im frankierten Umschlag absenden" (Fettdruck im Original). Die Angabe von Kontaktdaten ist nicht vorgesehen.

Durch die bundesrechtliche Regelung sehen wir uns in unserer Auffassung bestätigt, dass auch in Wahlangelegenheiten die Korrespondenz zwischen Staat und Bürger schon aus allgemeinen datenschutzrechtlichen Erwägungen nur verschlossen erfolgen sollte. Zumindest sollten die Betroffenen nicht durch staatliche Stellen unnötig dazu verleitet werden, bei Nutzung des Antragsvordrucks die gesetzlich

vorgeschriebenen und weitere freiwillige Angaben während des offenen Postversands unbefugten Dritten quasi aufzudrängen.

Um die Betroffenen zu sensibilisieren, haben wir uns mit einer Presseerklärung an die Öffentlichkeit gewandt.

Für die Bürgerschaftswahl 2012 würden wir eine Anpassung der Anforderungen an die Bundesregelung begrüßen. Im Übrigen werden wir die weitere Praxis kritisch verfolgen.

13.2 Rekrutierung von Schöffen und ehrenamtlichen Richtern

Bei Werbeaktionen für die Übernahme eines Ehrenamtes als Schöffe oder ehrenamtlicher Richter ist die Zweckbindung anderer Dateien zu beachten. Die Freiwilligkeit der Aktion muss auch bei der Datenerhebung zur weiteren Bearbeitung des Antrags deutlich werden.

Im Jahre 2008 stand die Rekrutierung von Schöffen und ehrenamtlichen Richtern für die verschiedenen Gerichtszweige an. Hierzu müssen auf Bezirksebene Wahllisten erstellt werden, die den Gerichten zur Wahl übersandt werden. Die Listen müssen jeweils doppelt soviel Vorschläge wie zu besetzende Plätze enthalten.

Anlässlich einer Eingabe erfuhren wir, dass ein Bezirksamt sich hierzu entgegen der Darstellung im Anschreiben nicht einer Stichprobe aus dem Melderegister bedient hatte, sondern dazu die Wahlhelferdatei der vorangegangenen Bürgerschaftswahl nutzte, um einzelne Bürger unter Fristsetzung anzuschreiben und sie zu einer Bewerbung zu bewegen. Beigefügt waren Auszüge aus der Verwaltungsgerichtsordnung und dem Gerichtsverfassungsgesetz, die den Eindruck vermittelten, dass eine Pflicht zur Übernahme des Ehrenamtes besteht, soweit keine gesetzlichen Hinderungsgründe entgegenstehen. Die Anfrage enthielt ein Antwortformular, nach dem man sein Einverständnis oder bei Ablehnung die Ablehnungsgründe benennen musste. Parallel dazu war ein Formular zum Vorliegen gesetzlicher Ausschlussgründe auszufüllen.

Mit dem Landeswahlamt bestand Einigkeit, dass eine Nutzung der Wahlhelferdatei nicht zulässig war. Hierfür waren die Betroffenen ausdrücklich schriftlich befragt worden, ob sie für künftige Wahlen zur Verfügung stehen wollten, und schriftlich belehrt worden, dass die Daten nur für diesen Zweck gespeichert würden und eine Weitergabe an Dritte nicht erfolge.

In der Nutzung zu Zwecken der Rekrutierung von Schöffen war eine Zweckänderung zu sehen, die von der Einwilligungserklärung nicht abgedeckt war. Dementsprechend waren die Angaben der Bürger, die sich nicht auf ein Schöffenamt bewerben wollten, zu löschen.

Unabhängig davon war jedoch auch die Art der vorsorglichen Datenerhebung über mögliche Ausschlussgründe datenschutzrechtlich bedenklich.

Schöffen werden gewählt aus einer Vorschlagsliste, auf die sie sich entweder selbst bewerben können oder aber von verschiedenen Organisationen vorgeschlagen werden können. Es besteht offenbar die Übung, diese Organisationen anzuhalten, vorab zu klären, ob Ausschlussgründe bei den Befragten bestehen.

Im vorliegenden Falle wurde jedoch der Eindruck erweckt, als könnten die Angeschriebenen schon in diesem Verfahrensstadium nur beim Vorliegen gesetzlicher Ausschlussgründe die Benennung ablehnen und als müssten die im Anhang auf-

gelisteten Fragen dafür beantwortet werden. Auf die Freiwilligkeit der Bewerbung und der erfragten Angaben wurde nicht hinreichend hingewiesen.

Wir haben deshalb gebeten, die Anschreiben für künftige Fälle so umzugestalten, dass der Charakter der unverbindlichen Anfrage deutlich zum Ausdruck kommt, dass eine Rückmeldung nur bei Interesse erforderlich sei und dass selbstverständlich auch die Zusatzfragen nur von denjenigen zu beantworten sind, die sich um ein Schöffenamt bewerben wollen.

14. Verkehr

14.1 Online-Projekt eDa KFZ

Mit dem Online-Projekt eDa KFZ wird die elektronische Vorbereitung von Zulassungsvorgängen weiter ausgebaut. Die Voraussetzungen für ein medienbruchfreies Verfahren sind nach wie vor nicht gegeben.

Nach dem Verfahren KFZ-Ummeldung (vgl. 21. TB, 17.3), das die elektronische Vorbereitung der Ummeldung durch KFZ-Halter selbst ermöglicht, wurde ein entsprechendes Verfahren entwickelt, mit dem nun ausgesuchte Großkunden (sog. Flottenbesitzer wie Versicherungen, aber auch größere Händler mit vielen Zulassungsvorgängen) auf der Grundlage einer schriftlichen Vereinbarung Anmeldungen und Stilllegungen vorbereiten können. Dazu werden Kennzeichen-, Fahrzeug, Halter-, Versicherungs- und Kontodaten vorab elektronisch an den Landesbetrieb Verkehr (LBV) übermittelt. Das Verfahren soll alle Beteiligten insbesondere in Spitzenlastzeiten entlasten. Für die endgültige Bearbeitung ist weiterhin ein unterschriebener schriftlicher Antrag, die Identifizierung durch Ausweispapiere sowie gegebenenfalls die Vorlage einer schriftlichen Vollmacht erforderlich.

Datenschutzrechtlich war zunächst zwischen Firmen, die die Vorgänge in eigener Sache anstoßen (Firmenwagen), und Händlern, die die Zulassung in Vollmacht für ihre Käufer als eigentliche KFZ-Halter anstoßen, zu unterscheiden. Firmen, die das Angebot in eigener Sache wahrnehmen, haben lediglich die Vereinbarung zu schließen.

Anders verhält es sich bei der Zulassung für die Kunden der Händler. Schon heute wird die weit überwiegende Mehrzahl der Anmeldungen durch schriftlich bevollmächtigte Händler vorgenommen. Soll das neue elektronische Verfahren genutzt werden, müssen im Zweifel auch mehr Kundendaten beim Händler elektronisch verarbeitet werden. Dies gilt insbesondere für die Kennziffer der elektronischen Versicherungsbescheinigung und für die für Kontodaten, da die Zulassung jetzt ausschließlich nach erteilter Einzugsermächtigung zugunsten des Finanzamts für Verkehrssteuern vorgenommen werden kann.

Auch wenn die elektronische Datenverarbeitung rechtlich ausschließlich das Innenverhältnis zwischen Käufer und Händler berührt, so wird die zusätzliche Datenverarbeitung durch das Serviceangebot des LBV doch zumindest animiert.

Wir haben deshalb besonderen Wert darauf gelegt, dass der Händler schon in der Nutzungsvereinbarung mit dem LBV verpflichtet wird, von seinem Kunden eine informierte Einwilligung in diese zusätzlich erforderliche Datenverarbeitung einzuholen und dabei auch über die dortigen Löschungsfristen aufzuklären, und gemeinsam ein entsprechendes Formular erarbeitet.

Technisch war sicherzustellen, dass alle Übermittlungen, also auch Fehlermeldungen, zwischen den Beteiligten verschlüsselt erfolgen.

14.2 Controllingsystem Bundesfernstraßenbau

Ein Verfahren, das die personenbezogene Auswertung von Ausschreibungs- und Abrechungsunterlagen aus dem Bereich des Bundesfernstraßenbaus zum Zwecke der Aufdeckung und Verhinderung von Korruption ermöglichen soll, bedarf einer hinreichenden bundesgesetzlichen Grundlage.

Im Sommer 2008 wurden die Länder durch den Bundesbeauftragten für Datenschutz und Informationsfreiheit an der Beurteilung eines Verfahrens „Controllingsystem Bundesfernstraßenbau" des Bundesministeriums für Verkehr, Bau und Stadtentwicklung beteiligt.

Nach den Unterlagen sollte ein System entwickelt werden, das eine wirksame Korruptionsbekämpfung als Frühwarnsystem über von der Verwaltung zu definierende Parameter gewährleisten sollte. Dafür sollten der Bundesverwaltung alle Verfahren zentral gemeldet und dort zentral ausgewertet werden. Dazu konnte und sollte auf das Merkmal „Marktteilnehmer" jeweils nicht verzichtet werden. Eine dort nur pseudonyme Verarbeitung wurde nicht für ausreichend gehalten. Als Rechtsgrundlage wurden Artikel 85 des Grundgesetzes (GG), eine noch zu schließende Verwaltungsvereinbarung zwischen Bund und Ländern sowie die allgemeinen Datenverarbeitungsvorschriften der Landesdatenschutzgesetze benannt.

Von datenschutzrechtlicher Relevanz sind dabei nur diejenigen Firmen, die als Inhaberfirma oder Personengesellschaft geführt werden, vorliegend in erheblichem Umfang insbesondere Ingenieurbüros. Daneben sind aber auch in empfindlicher Weise die beteiligten Sachbearbeiter der Straßenverkehrsverwaltungen betroffen. Die Verarbeitung personenbezogener Daten dieser Betroffenen steht unter dem Gesetzesvorbehalt und hat dem Bestimmtheitsgrundsatz zu genügen. Danach müssen die Betroffenen aus materiellen Gesetzen entnehmen können, welche Daten von ihnen zu welchen Zwecken in welcher Form verarbeitet werden dürfen.

Hinzu kommt, dass für Hamburg die Beteiligung an einer länderübergreifenden Verbunddatei aufgrund von § 11 a des Hamburgischen Datenschutzgesetzes (HmbDSG) nicht im Wege der Verwaltungsvereinbarung, sondern nur auf der Grundlage eines Staatsvertrags in Betracht kommt.

In unserer Stellungnahme haben wir darauf hingewiesen, dass ein solches Vorgehen einen besonders tiefen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen beinhaltet und bisher nur auf der Grundlage von ausdrücklichen gesetzlichen Regelungen zur Korruptionsbekämpfung erfolgen darf. Typischerweise stützen sich solcherart Register auf nachgewiesene Vorwürfe nach abgeschlossenem Verfahren. Hier sollten als Maßstab jedoch schon Annahmen der Bundesverwaltung, wie ein bestimmtes prozentuales Überschreiten von Durchschnittswerten, ausreichen.

Eine weitere Diskussion konnte uns nicht davon überzeugen, über eine Landesverordnung nach § 11 a HmbDSG den Weg für eine zulässige Datenverarbeitung bei der Bundesverwaltung freizugeben: Eine Verordnung nach § 11 a HmbDSG kann nur die besondere Form der Datenverarbeitung regeln, setzt aber eine hinreichende materielle Übermittlungsbefugnis voraus, die in diesem Bereich nur durch den Bundesgesetzgeber erlassen werden kann.

Seit Jahren wird auch in anderen Bereichen für eine wirksame Korruptionsbekämpfung über Ländergrenzen hinweg ein Bundes-Korruptionsbekämpfungsgesetz für erforderlich gehalten, das jedoch noch aussteht.

15. Wirtschaftsverwaltung

15.1 Beteiligung privater Banken an Subventionsvergabe

Werden private Banken oder sonstige Dritte an der Bearbeitung von Subventionsanträgen beteiligt, so sind die datenschutzrechtlichen Grenzen zwischen Auftragsdatenverarbeitung und Funktionsübertragung zu beachten. Im Bereich der Mittelstandsförderung ist die neue Datenschutzregelung einzuhalten.

Ende 2008 wurden uns von der Behörde für Wirtschaft und Arbeit zwei automatisierte Verfahren zur Subventionsbewilligung im Mittelstandsbereich nach Landesrecht vorgelegt.

Seit den fünfziger Jahren bestand die Praxis, solche Subventionen von der Bürgschaftsgemeinschaft GmbH (BG), später auch von der Beteiligungsgesellschaft mbH (BTG) bearbeiten zu lassen. Beides sind Selbsthilfeorganisationen der Wirtschaft. Die letztliche Bewilligung erfolgte, auch wegen teilweiser Beteiligung von Bundesmitteln, durch die bei der Wirtschaftsbehörde angesiedelte Kreditkommission. Allerdings wurden ihr Fälle zur Ablehnung nicht vorgelegt; vielmehr haben über mangelnde Erfolgsaussichten ausschließlich die Institute selbst befunden. Die Behörde bezeichnete dies als Auftragsdatenverarbeitung. Wir haben dies beanstandet.

Bei den Subventionen handelt es sich um öffentlichrechtliche Leistungen, über die per Zuwendungsbescheid zu entscheiden ist. Dabei fallen eine Vielzahl empfindlicher personenbezogener Daten an, wie dies das Verfahren BG intensiv!, das als Umstrukturierungsprogramm für mittelständische Unternehmen in Schwierigkeiten konzipiert ist, nachdrücklich belegte. Bei den Betroffenen handelte es sich auch ganz überwiegend um Personengesellschaften, die dem Schutz des Hamburgischen Datenschutzgesetzes unterfallen.

Eine Auftragsdatenverarbeitung nach § 3 des Hamburgischen Datenschutzgesetzes (HmbDSG) liegt nur solange und soweit vor, als der Auftragnehmer mit technischen Unterstützungsleistungen zur Abwicklung der Anträge betraut wird. Darüber hinaus kann eine Auftragsdatenverarbeitung auch dann vorliegen, wenn im Einzelfall gutachtlicher Sachverstand eingekauft wird. Grundsätzlich hat eine Behörde den erforderlichen Fachverstand für die ihr übertragenen Aufgaben jedoch selbst vorzuhalten. Werden ganze Programme zur inhaltlichen Bearbeitung übertragen, so handelt es sich nicht mehr um eine bloße Auftragsdatenverarbeitung, sondern um eine Funktionsübertragung, für die eine Beleihung vorgenommen werden muss.

Mit der Behörde waren wir einig, dass es insbesondere im Falles des Programms BG intensiv! einer solchen Beleihung bedarf.

Im Juli 2009 wurde deshalb eine Datenverarbeitungsvorschrift in § 21 Mittelstandsförderungsgesetz (MFG) aufgenommen, nach der komplette Verwaltungsaufgaben im Wege der Beleihung vergeben werden dürfen, die Beurteilung einzelner Fördervoraussetzungen kann, soweit dies in den einschlägigen Richtlinien geregelt wird, im Wege des Auftrags vergeben werden.

Zur Beleihung der BG für das Programm BG intensiv! war wegen der Einbindung von EU-Fördermitteln auch eine europaweite Ausschreibung erforderlich.

Auf Nachfrage erklärte die Behörde zu Redaktionsschluss jedoch, dass das Programm zur Zeit komplett im Wege der Auftragsdatenverarbeitung mit der Vergabe von bis zu 3 Teil-Gutachten pro Fall nebst der anfallenden Datenverarbeitung betrieben würde und wahrscheinlich auch 2010 in dieser Form weitergeführt würde.

Wir haben die Behörde um nähere Angaben gebeten, um beurteilen zu können, ob hierin ein Unterlaufen des § 21 MFG zu sehen ist oder ob dies noch als Übergangslösung zu einem datenschutz- und europarechtskonformen Verfahren hingenommen werden kann.

15.2 Modernisierung des Gewerberegisters

Die seit langem geplante Modernisierung des Gewerberegisters bei gleichzeitiger Erweiterung um neu zugelassene elektronische Übermittlungen bedarf bei Einsatz verschiedener Systemkomponenten sorgfältiger Planung. Angesichts der Bedeutung des Gewerberegisters für die Betroffenen ist der Test in einer funktionierenden Testumgebung von überragender Bedeutung. Eine Einbindung der Handelskammer darf nur entsprechend ihrem engen Auftrag erfolgen.

Seit Jahren wurde eine Modernisierung des alten Gewerberegisters vorbereitet. Dabei handelt es sich nicht um ein Register im eigentlichen Sinne, sondern um die althergebrachte Bezeichnung für die Vorgangsverwaltung der Gewerbeüberwachung, die auch die gesamte Historie der angemeldeten Gewerbebetriebe enthält. Mit dem Zweiten Mittelstandsentlastungsgesetz (2.MEG) wurden umfangreiche Regelungen zur Datenübermittlung aus den Gewerbeanzeigen neu gefasst. Dies gilt es, gleichzeitig umzusetzen. Daneben wurde die Handelskammer per Zuständigkeitsanordnung mit der Entgegennahme der Gewerbeanzeigen nach § 14 Gewerbeordnung (GewO) und der Ausgabe der Bestätigung nach § 15 GewO beauftragt. Abweichend von den Bezirken, die nur im Rahmen ihrer örtlichen Zuständigkeit Zugriff haben werden, ist die Kammer für das gesamte Stadtgebiet zuständig. Zu berücksichtigen ist weiter eine wenig durchschaubare spezifische Zuständigkeitsregelung in der GewO, die gleichwohl nur im Lichte der Übermittlungsregelungen des Hamburgischen Datenschutzgesetzes (HmbDSG) auszulegen ist. Schließlich soll auch noch ein eigenes eGovernment-Angebot zur elektronischen Gewerbeanzeige integriert werden.

Zur Umsetzung dieser Vorhaben wurden zwei Projekte mit jeweiligen Unterprojekten (Fachverfahren mit migewa und migewaView; Online-Verfahren mit e-Auskunft und Gewerbemeldung-online) ins Leben gerufen, die sich jedoch in vielen Bereichen überschneiden.

Wir haben verschiedene Informationsgespräche geführt und haben für den Bereich des eigentlichen Fachverfahrens nach der unverbindlichen Präsentation eines Anbieters kurz vor Produktivsetzung eine erste Risikoanalyse und Verfahrensbeschreibung zugeleitet bekommen. Man hat sich für ein mehrmoduliges Standardverfahren entschieden, dessen Inhalte im einzelnen noch nicht dargestellt wurden. Sachbearbeiter mit schreibendem Zugriff auf ein Modul haben ausnahmslos Zugriff auf alle darin enthaltenen Daten. Das Modul migewaView erlaubt ausschließlich den lesenden Zugriff, ermöglicht hierbei die Abfrage des Verwendungszwecks und kann auch eingeschränkte Zugangsberechtigungen abbilden.

Hier kommt es wesentlich darauf an, dass nur solche Stellen bzw. Mitarbeiter, die unmittelbar und umfassend mit der Gewerbeüberwachung im engeren Sinne betraut sind, Zugriff auf das Register in dem für sie erforderlichen Umfang erhalten. Dabei wird statt des gesetzlich privilegierten Abrufverfahrens ein Zugriff über eine Portallösung favorisiert.

Daneben gilt es, die in § 14 Absatz 9 GewO genannten dritten öffentlichen Stellen, die regelhaft Daten aus der Gewerbeanzeige für eigene Zwecke erhalten, durch die Einrichtung von Abrufverfahren komfortabler mit den jeweils aktuellen Daten aus dem Gewerberegister zu versorgen und die Berechtigung auf die dort für jede Stelle genau benannten Daten zu beschränken.

Besondere Beachtung muss die Anbindung der Handelskammer erfahren. Sie tritt in dem Verfahren in drei verschiedenen Rollen auf: Als abrufberechtigte öffentliche Stelle zur Aufgabenwahrnehmung in eigenen Angelegenheiten, als zuständige Stelle zur Entgegennahme der Anzeigen und schließlich als einheitlicher Ansprechpartner im Sinne der EU-Dienstleistungsrichtlinie als Zuträger zwischen Betroffenem und zuständiger Behörde.

In eigener Sache darf sie die aktuellen Gewerbeanzeigendaten zu Selbstverwaltungszwecken abrufen, als zuständige Stelle darf sie die aktuellen Anzeigendaten einsehen und die Bescheinigung nach § 15 GewO ausstellen. Dies muss technisch ohne einen Zugriff auf die sonstigen Daten des Registers umgesetzt werden. Als Zuträger kommt der Kammer ebenfalls keine eigene Bearbeitungsbefugnis zu.

Seit dem 2. MEG dürfen Name, betriebliche Anschrift und die angezeigte Tätigkeit allgemein zugänglich gemacht werden. Wird hierfür ein Abrufverfahren auch für Firmen und private Dritte eingerichtet, so ist entweder der Name oder die betriebliche Anschrift anzugeben. Dabei kann entweder die Abfrage mit unvollständigen Daten zugelassen werden oder die Suche mit Ähnlichenfunktion, das heißt mit einer Vielzahl von Treffern, die ähnliche Daten betreffen. Eine kumulative Ausgestaltung ist nach dem Wortlaut ausgeschlossen.

Ebenfalls beachtlich ist, dass für Privatbetriebe eine Übermittlung weiterer Daten aus der Gewerbeanzeige nur zulässig ist, wenn sie glaubhaft machen, daran ein rechtliches Interesse zu haben. Dies kann entgegen dem leicht missverständlich formulierten § 14 Absatz 8 GewO nur im Wege einer verantwortlichen Einzelfallprüfung erfolgen, so dass ein automatisierter Abruf denknotwendig ausgeschlossen ist.

Die uns vorliegenden ersten Überlegungen für ein online-Verfahren zur Abgabe von Gewerbeanzeigen, also An-, Um- und Abmeldungen, beschreiben zwar die Verfahrensabläufe, berücksichtigen aber noch nicht die spezifischen Anforderungen an Vertraulichkeit, Authentizität und Revisionsfähigkeit des Verfahrens.

So sollen für Um- und Abmeldungen die aktuellen Daten angezeigt werden und ein schreibender Zugriff gewährt werden

Die elektronische Abgabe von Gewerbeanzeigen ist in der GewO noch nicht vorgesehen. Das Verfahren muss daher den Anforderungen des Hamburgischen Datenschutzgesetzes (HmbDSG) entsprechen. Die direkte Eingabe eigener Daten durch den Betroffenen in ein Fachverfahren ist darin nicht vorgesehen. Es kennt in § 11 a HmbDSG lediglich die Eingabe und Verarbeitung durch mehrere Daten verarbeitende Stellen. Dies sind gemäß § 4 Absatz 3 HmbDSG ausschließlich öffentliche Stellen, die von dessen Geltungsbereich umfasst sind. Es ist daher technisch si-

cherzustellen, dass die Daten des Betroffenen nicht unmittelbar in das Fachverfahren gelangen, sondern erst nach Prüfung durch einen zuständigen Sachbearbeiter eingestellt werden. Auch das setzt jedoch voraus, dass der Betroffene zweifelsfrei identifiziert werden kann. Dies ebenso wie die Einhaltung der gesetzlich vorgesehenen Schriftform ist bisher nur durch eine qualifizierte elektronische Signatur des Betroffenen für den Zeitpunkt der Übermittlung gewährleistet. Hinzu kommt aber, dass, soll die Identität des Anzeigenden dauerhaft nachweisbar sein – und dies ist in Bereichen des Verbots mit Erlaubnisvorbehalt der Fall – gemäß § 1 Absatz 3 des Signaturgesetzes weitere Anforderungen an eine Signatur zu formulieren sind und dies am Datensatz selbst und nicht in einer kurzlebigen log-Datei zu dokumentieren ist.

Zusätzlich ist eine verschlüsselte Übermittlung zu gewährleisten.

Technisch-organisatorische Überlegungen liegen uns erst für das Fachverfahren und für eine erste Stufe vor.

Die Nutzung eines Sharepoints für originäre Überwachungsaufgaben begegnet keinen Bedenken, wenn die Zugriffsrechte aufgabenbezogen abgebildet und protokolliert werden.

Die erforderlichen technischen und organisatorischen Maßnahmen müssen noch in der Risikoanalyse dargelegt werden.

Ein nicht zu heilender Datenschutzverstoß liegt bereits vor, indem der Testbetrieb vor Übernahme in die Produktivumgebung entgegen den Vorschriften der Freigaberichtlinie ausschließlich mit Echtdaten betrieben wurde.

Gefordert ist eine Testumgebung, in der mit Testdaten gearbeitet wird und in der nur unter engen, zu dokumentierenden Ausnahmefällen auf Echtdaten zurückgegriffen werden darf.

Für die weitere Anwendung haben wir kurzfristig den Aufbau einer normgerechten Testumgebung gefordert.

15.3 Videoüberwachung der Spielbank Hamburg zu aufsichtlichen Zwecken

Eine lückenlose Videoüberwachung der Spielbankbesucher und ihrer Mitarbeiter bei gleichzeitiger elektronischer Protokollierung der Automatennutzung ist auch bei einer spezialgesetzlichen Regelung verfassungsrechtlich bedenklich. Wird die Überwachung zu Zwecken der Spielaufsicht und Steueraufsicht angeordnet, so darf hierfür nicht eine vorhandene private Anlage mitgenutzt werden.

Im Sommer 2009 wurde uns im Rahmen des Gesetzgebungsverfahrens zur Novellierung des Spielbankgesetzes erstmals das Vorhaben bekannt, in der Spielbank Hamburg, einer Kommanditgesellschaft, ein Videoüberwachungssystem vorzuschreiben, mit dem eine flächendeckende Überwachung einschließlich Aufzeichnung der Spielbankbesucher und ihrer Mitarbeiter in den Spielsälen sowie weiterer interner Bereiche angeordnet werden sollte. Sie sollte auch die Gesichtserkennung bei schummrigen Lichtverhältnissen gewährleisten. Dies sollte vorrangig weniger zum Schutz der Spieler als vielmehr zur Einsparung von Personalaufwendungen der Aufsichtsbehörden erfolgen. Als weitere Argumente wurden die Richtigkeit der Besteuerungsgrundlage angeführt sowie die Möglichkeit, unbefugten Spielern das unbefugte Betreten nachzuweisen, so dass Regressforderungen gegen die Spielbank abgewehrt werden könnten.

Bisher werden die Spielaufsicht und die Steueraufsicht in der Spielbank durch Behördenmitarbeiter wahrgenommen, die von der Vorbereitung der Spieltische über die Beobachtung des Spielablaufs bis zur Kassenabrechnung die Abläufe in der Spielbank überwachen. Dies geschieht zurzeit bereits unter der Beobachtung einer umfassenden Videoüberwachung von über 160 Kameras, die die Spielbank allein im Standort Esplanade für eigene Zwecke und zum Teil aufgrund von Arbeitsschutzvorschriften betreibt.

In den meisten Bundesländern sind entsprechende Regelungen zur Videoüberwachung der dortigen Spielbanken in unterschiedlicher Intensität bereits verabschiedet worden.

Der vorgelegte Entwurf lehnte sich eng an eine Regelung von Mecklenburg-Vorpommern an; anders als in Hamburg war dort das Land Betreiber der Spielbank.

Ungeachtet dessen, dass Spielbanken als Ort der Geldwäsche allgemein bekannt sind, haben wir aus folgenden Gründen gleichwohl erhebliche Bedenken gegen die geplanten Regelungen angemeldet:

Die Videoüberwachung greift in besonderem Maße in einen empfindlichen Teil der Freizeitgestaltung der betroffenen Besucher ein und überwacht die Mitarbeiter während ihrer gesamten Arbeitszeit. Die ganz überwiegende Mehrzahl der Betroffenen dürfte sich gesetzeskonform verhalten. In diesem Falle kommt eine Überwachung nur dann in Betracht, wenn öffentliche Interessen die Interessen der Betroffenen deutlich überwiegen und keine milderen Mittel für die Erreichung des Zwecks zur Verfügung stehen.

Abgesehen davon, dass für verschiedene Vorgehensweisen, insbesondere den Einsatz von Strohmännern und -frauen, die Videoüberwachung kein geeignetes Mittel zum Erreichen der Steuerehrlichkeit ist, ist auch gerade im Bereich der Suchtprävention ein direktes Ansprechen der Betroffenen effektiver, sei es bei der Zutrittskontrolle oder am Spieltisch. Für Zwecke der Strafverfolgung fehlt es dem Landesgesetzgeber an der Regelungskompetenz.

Mit dem Gesetz sollte die Spielbank Hamburg verpflichtet werden, privat betriebene Anlagen auch zu Aufsichtszwecken zu betreiben und den Aufsichtsbehörden uneingeschränkten Zugang zu den Daten zu verschaffen. Damit wird eine gemeinsame Datenverarbeitung mit einer privaten Stelle angeordnet, die noch dazu das Objekt der behördlichen Aufsicht darstellt. Eine gemeinsame Datei mit Privaten ist schon allgemein nach den Vorschriften des Hamburgischen Datenschutzgesetzes (HmbDSG) nicht zulässig.

Wir begrüßen, dass nach eingehender Diskussion die Novellierung des Spielbankgesetzes ohne die problematisierten Bestimmungen über die Videoüberwachung erfolgt ist.

16. Ausländerwesen

16.1 Zweite Prüfung zur ausländerrechtlichen Ausschreibung im Schengen-Informationssystem SIS

Eine sachgerechte Prüfung der Speicherfristen im SIS kann nur im Zusammenwirken von Ausländerbehörden und Bundeskriminalamt erfolgen. Anlassbedingte Änderungsmitteilungen können die Belange der Betroffenen sicherer schützen als regelhafte Prüfungen durch die Ausländerbehörden.

Ausschreibungen nach Art. 96 des Schengen Durchführungsübereinkommens (SDÜ) zur Wiedereinreiseverweigerung von Drittausländern machen ca. 90 % der Ausschreibungen im SIS aus. Zweck des Systems ist es nach Wegfall der innereuropäischen Grenzkontrollen unter anderem, die Einhaltung der ausländerrechtlichen Einreisebeschränkungen an den Außengrenzen sicherzustellen. Die Ausschreibungen werden von den Ausländerbehörden über die zuständigen Landeskriminalämter (LKA) veranlasst und verantwortlich durch das Bundeskriminalamt (BKA) in das europaweite System übermittelt. Bereits im Jahre 2004 hatte die Gemeinsame Kontrollinstanz für Schengen (GK) eine europaweit koordinierte datenschutzrechtliche Prüfung initiiert. Defizite ergaben sich in Deutschland vor allem bei den Fragen zur Dokumentation der Ausschreibungsvoraussetzungen und zur Einhaltung von Überprüfungs- und Löschungsfristen. Artikel 112 SDÜ regelt, dass eine Speicherung nicht länger als für den verfolgten Zweck erforderlich erfolgen darf. Spätestens drei Jahre nach Einspeicherung ist die Erforderlichkeit der weiteren Speicherung von der ausschreibenden Vertragspartei zu prüfen. Artikel 104 SDÜ regelt ergänzend, dass das nationale Recht gilt, soweit nicht das Übereinkommen engere Voraussetzungen für die Ausschreibung enthält.

Im Mai 2008 wurde eine zweite Nachfolgeprüfung mit denselben Fragestellungen durchgeführt. Ziel war es zu klären, ob die seinerzeit festgestellten Defizite behoben worden seien. In diesem Zusammenhang wurden insgesamt 46 Fälle überprüft. Im Ergebnis sind zutreffend nur noch Drittausländer und nur bei vorliegender Abschiebungs- bzw. Ausreiseverfügung zur Meldung an das LKA weitergeleitet worden. Nach § 11 Aufenthaltsgesetz (AufenthG) gelten die Verbote lebenslang, können aber auf Antrag verkürzt werden. Dementsprechend waren in den Vorgängen Aktualisierungsmeldungen bei nachträglichen Befristungen oder Ehegattenzuzug vorgenommen worden. Längerfristige Speicherungen ergaben sich zum Teil aus neueren Meldungen durch Drittstaaten, zum Teil durch die sehr komplizierte Zuordnung bei mehreren Aliaspersonalien. Der Ausschreibungsantrag an das LKA war jeweils noch in der Akte enthalten.

Nur lückenhaft waren Prüfentscheidungen nach drei bzw. sechs Jahren Speicherung dokumentiert.

Die Ausländerbehörde berief sich auf die lebenslange Wirkung des Wiedereinreiseverbots und verwies auf ihre Praxis der Aktualisierungsmeldungen. Ergänzend wies sie darauf hin, dass es ein bundesweit mit dem BKA abgestimmtes Verfahren gebe, wonach nach drei Jahren eine Erinnerungsmitteilung vom BKA erfolgt, nach der die weitere Speicherung automatisch um weitere drei Jahre verlängert würde, soweit die Ausländerbehörde keine anderweitige Entscheidung mitteile; nach insgesamt sechs Jahren Speicherung enthalte die Mitteilung den Hinweis, dass die Eintragung gelöscht werde, soweit nichts Entgegenstehendes mitgeteilt werde.

Nach unserer Auffassung ist diese Vorgehensweise datenschutzrechtlich vertretbar. Nach § 112 SDÜ erfolgt die Speicherung, solange sie erforderlich ist. Dies ist nach § 11 AufenthG lebenslang. Die regelmäßige Pflicht zur Überprüfung der Speicherung berührt die Erforderlichkeit der Speicherung nicht.

Die verantwortliche Überprüfung der Speicherfrist obliegt dem BKA als nationaler meldender Stelle. Mit dem gewählten Verfahren dürfte eine datenschutzgerechte Überprüfung jedenfalls dann hinreichend gewährleistet sein, wenn, wie in Hamburg praktiziert, parallel Änderungsmitteilungen vorgenommen werden. Eine regelhafte Löschung nach sechs Jahren trotz weiterbestehenden Einreiseverbots ist

eine fachliche Entscheidung, die Datenschutzbelange der Betroffenen nicht negativ berührt.

Im Hinblick auf die Dauerwirkung des Einreiseverbots ist die weitere Speicherung der Meldung in der Ausländerakte selbst nicht zu beanstanden (Aktenprivileg nach § 19 Abs. 3 Hamburgisches Datenschutzgesetz).

In diesem Sinne haben wir den Hessischen Datenschutzbeauftragten als Vertreter der GK unterrichtet und angeregt, gegebenenfalls das bundesweite Verfahren zu optimieren.

16.2 Datenschutzrechtliche Belange von Verpflichtungsgebern und der Gesetzentwurf zur Visa-Einlader- und Warndatei

Erklären sich Bürger und Institutionen bereit, den Unterhalt für den Inlandsaufenthalt eines Ausländers sicherzustellen, so haben sie nicht nur weitgehende Auskünfte über ihre persönlichen und wirtschaftlichen Verhältnisse abzugeben, sondern sollen auch noch in einer geplanten bundesweiten Einladerdatei geführt werden, die zur Vermeidung von Visamissbräuchen und zur Nutzung durch Polizei- und Strafverfolgungsbehörden sowie der Nachrichtendienste zur jeweiligen Aufgabenwahrnehmung zur Verfügung stehen soll.

Bereits in der Vergangenheit haben sich die Datenschutzbeauftragten intensiv mit der Praxis der Datenerhebung bei sogenannten Verpflichtungsgebern beschäftigt.

Kann ein Ausländer seinen Aufenthalt im Bundesgebiet nicht aus eigenen Mitteln bestreiten, so besteht grundsätzlich kein Anspruch auf Einreise. Die fehlende Leistungsfähigkeit kann durch Beibringung einer sogenannten Verpflichtungserklärung ersetzt werden. Darin verpflichtet sich ein Dritter, für die Dauer des Aufenthalts für den Lebensunterhalt einschließlich etwaiger Krankheits- und Pflegekosten aufzukommen.

Zwar ist das Instrument der Verpflichtungserklärung in § 67 Aufenthaltsgesetz geregelt, nicht aber die dafür erforderliche Datenverarbeitung. Die Betroffenen werden daher auf die Freiwilligkeit ihrer Angaben hingewiesen. Nähere Regelungen enthalten die danach erlassenen Allgemeinen Verwaltungsvorschriften zum Aufenthaltsgesetz sowie weitere Anwendungshinweise. Als untergesetzliche Regelungen haben sie keinen grundrechtseinschränkenden Charakter.

Trotz datenschutzrechtlicher Einwilligung ist das Übermaßverbot zu beachten und die Erforderlichkeit daher nach den allgemeinen Datenverarbeitungsvorschriften des Hamburgischen Datenschutzgesetzes zu beurteilen. Entsprechend der Vielfalt der Lebenssachverhalte ist eine generelle Regelung schwierig. Die Überprüfung der hamburgischen Praxis hatte seinerzeit je nach Dienststelle teilweise abweichende Vorgehensweisen ergeben. Einzelne Datenschutzhinweise waren gegeben worden.

Als problematisch war darüber hinaus erkannt worden, dass die zuständigen Stellen nicht immer vom Vorliegen einer Verpflichtungserklärung erfahren. Eine hamburgische Regelung war im Hinblick auf eine angestrebte Regelung im Ausländerzentralregistergesetz zurückgestellt worden.

Im Februar 2009 erreichte uns ein Referentenentwurf zur Errichtung einer Visa-Einlader- und Warndatei, den wir den übrigen Ländern zur Kenntnis gegeben haben.

Ziel war es, präventiv und repressiv Visaerschleichungen und damit in Zusammenhang stehende Straftaten zu bekämpfen und zu verhindern.

Zu diesem Zweck sollte eine bundesweite Visawarndatei errichtet werden, in der nicht nur erkannte Missbrauchsfälle, sondern auch Verdächtige sowie insbesondere die Grunddaten aller Einlader und Verpflichtungsgeber enthalten sein sollten. Diese Daten sollten weiten Bereichen der Ordnungsverwaltung, der Justiz und den Nachrichtendiensten zur Verfügung stehen.

Es ergaben sich insbesondere verfassungsrechtliche Bedenken hinsichtlich der verdachtsunabhängigen Speicherung. So wurden neben den Verpflichtungsgebern auch die Mitarbeiter von Stellen, die einen internationalen Austausch fördern, unterschiedslos erfasst. Problematisch erschien auch die Übermittlung an Träger der Sozialhilfe und der Grundsicherung, die wohl in der Prüfung der Leistungsfähigkeit begründet sein sollten, aber nicht vom Gesetzeszweck abgedeckt waren.

Die Abstufung der Übermittlungstatbestände war aus sich heraus nicht normenklar.

Insgesamt verließ der Entwurf die Funktion als Visa-Warndatei. Der weit gefasste Berechtigtenkreis, fehlende Zweckbindung und breit eingeräumte Abrufmöglichkeiten waren umso problematischer zu sehen, als auch ungesicherte Tatsachen und Bagatellfälle Grundlage der Meldung sein sollten. Schließlich begegnete die Einschränkung der Betroffenenrechte datenschutzrechtlichen Bedenken.

Der Entwurf hat in der 16. Legislaturperiode keine Mehrheit im Bundestag gefunden, soll aber in der laufenden Periode neu eingebracht werden. Wir werden den weiteren Verlauf kritisch begleiten.

17. Meldewesen

Bundesmeldegesetz

Der Entwurf eines Bundesmeldegesetzes war die Chance, das Melderecht datenschutzfreundlicher zu gestalten. Im Entwurf des Bundesinnenministeriums wurde diese Chance nicht ergriffen.

Im Zuge der Föderalismusreform im Jahre 2006 wurde dem Bund die ausschließliche Gesetzgebungskompetenz für das Meldewesen übertragen. In der Folge entwickelte das zuständige Bundesinnenministerium den Entwurf eines Bundesmeldegesetzes, das die bisherigen Landesmeldegesetze ersetzen soll und mit dem ein einheitliches Melderecht in der Bundesrepublik geschaffen wird. Leider wurde dabei die Gelegenheit versäumt, ein modernes, den datenschutzrechtlichen Prinzipien verpflichtetes Melderecht zu schaffen, das dem Bürger mehr Rechte als bisher einräumt. Vielmehr wurden unzulängliche Regelungen, wie zum Beispiel die sogenannte einfache Melderegisterauskunft, nicht nur beibehalten, sondern erweitert (die einfache Melderegisterauskunft soll um die Daten Sterbetag und Sterbeort erweitert werden). Es soll dabei bleiben, dass jeder ohne Angabe von Gründen die Adressdaten einer bestimmter Person bekommen kann, ohne dass der Betroffene dagegen Widerspruch einlegen könnte oder auch nur informiert wird. Nach unserer Meinung ist die Beibehaltung solcher Regelungen in einer Zeit, in der der Adresshandel ein florierendes Geschäft ist, nicht nachvollziehbar. Zur Wahrung des informationellen Selbstbestimmungsrechts muss ein Meldepflichtiger die Möglichkeit haben, entweder von Anfang an gegen die Weitergabe der eigenen Daten

Widerspruch einzulegen oder in die Weitergabe seiner Daten an Dritte einzuwilligen.

Das Hamburgische Meldegesetz (HmbMG) kennt, im Gegensatz zu vielen anderen Landesmeldegesetzen, die Einwilligungsregelung schon aus den §§ 35 Absatz 2 und Absatz 3 HmbMG, in denen geregelt ist, dass Auskünfte an Parteien und Wählervereinigungen vor der Wahl zur hamburgischen Bürgerschaft und Auskünfte zu Alters- und Ehejubiläen nur erteilt werden dürfen, wenn der Betroffene in die Auskunftserteilung einwilligt. Diese Regelung ermöglicht es dem Meldepflichtigen frei darüber zu entscheiden, ob seine Daten für die genannten Zwecke weitergegeben werden dürfen. Leider wurden diese Regelungen im Entwurf des Bundesmeldegesetzes nicht übernommen. Das Bundesinnenministerium hat sich in seinem Entwurf für die Übernahme der ungünstigeren Regelung des § 22 Absatz 2 Melderechtsrahmengesetz (MRRG) und den entsprechenden Regelungen anderer Landesmeldegesetze entschieden, nach der die Daten der Betroffenen weitergegeben werden können, wenn sie dem nicht widersprechen. Auf diese Möglichkeit des Widerspruchs wird in der Regel im Falle der Alters- und Ehejubiläen einmal im Jahr durch öffentliche Bekanntgabe aufmerksam gemacht. Zwischen dieser öffentlichen Bekanntgabe und dem tatsächlichen Ereignis und damit dem Auskunftsersuchen, z.B. einer Tageszeitung, könnten unter Umständen also Monate liegen, in denen der Betroffene die Möglichkeit des Widerspruchs schlicht vergisst. Wenn diese Regelungen des Entwurfes des Bundesmeldegesetzes tatsächlich in Kraft treten sollte, würde sie zu einer deutlichen Einschränkung des informationellen Selbstbestimmungsrechts der meldepflichtigen Bürger Hamburgs führen. Dieser Umstand ist nicht tragbar, daher fordert der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ein Bundesmelderecht, das Widerspruchs-, Einwilligungs- und Auskunftsrechte für den Meldepflichtigen beinhaltet, die das informationelle Selbstbestimmungsrecht des Bürgers nachhaltig stärken.

18. Personalausweis- und Passwesen

18.1 Antragsverfahren für Reisepässe nicht sicher genug

Die biometrischen Daten werden bei der Beantragung von Reisepässen nicht mit den weiteren Antragsdaten verbunden, so dass ein Austausch dieser Daten möglich wäre. Die Löschung der Passantragsdaten entspricht nicht den gesetzlichen Anforderungen.

In den Kundenzentren der Einwohnerämter der Bezirke wird die Beantragung von Reispässen mit dem IT-Verfahren OK.EWO technisch unterstützt. Seit dem 1. November.2007 werden dazu neben dem Passbild auch erstmals die Fingerabdrücke von zwei Fingern als zusätzliche biometrische Daten des Antragstellers verarbeitet. Wir haben dieses IT-Verfahren, das für die Nutzung der biometrischen Daten erweitert wurde, im Herbst 2008 im Bezirksamt Hamburg-Mitte geprüft. Obwohl mit der Erweiterung offensichtlich wesentliche Änderungen verbunden sind, die im Vorfeld der Einführung und im Gesetzgebungsverfahren auch breit und kontrovers behandelt wurden, haben es die Daten verarbeitende Stelle und die Fachliche Leitstelle versäumt, die erforderliche Risikoanalyse zu erstellen und dem HmbBfDI zur Stellungnahme zuzuleiten. Ziel einer solchen Betrachtung vor der Einführung einer wesentlichen Verfahrensänderung ist es gerade, aus den spezifischen Risiken die erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen abzuleiten. Da diese Betrachtung durch die Fachliche Leitstelle, die zur Abteilung IT-Angelegenheiten der Bezirksverwaltung N/ITB gehört, ausblieb, verwundert es nicht,

dass bei der Prüfung durch den HmbBfDI zwei gravierende Mängel festgestellt wurden, die sich auf die Verarbeitung der Fingerabdruckdaten beziehen.

Die Verarbeitung der Fingerabdruckdaten haben das Ziel, den Passinhaber eindeutig identifizieren zu können. Dieses Ziel kann nur erreicht werden, wenn alle Daten zu einem Passantrag unmittelbar nach der Erfassung so miteinander verbunden werden, dass sowohl eine gewollte als auch ungewollte Veränderung sowie ein Austausch einzelner Daten technisch ausgeschlossen werden. Diese Kopplung aller Passantragdaten erfolgt derzeit nicht. Während des Beantragungsprozesses könnten so die Fingerabdruckdaten einer anderen Person den weiteren Antragsdaten wie Name, Anschrift und Passbild in der Datenbank von OK.EWO zugeordnet werden. Weder Sachbearbeitung noch Administratoren könnten bei einem Vorwurf der Manipulation das Gegenteil nachweisen. Wir haben auf die Möglichkeit hingewiesen, dass beispielsweise mit einer elektronischen Signatur die Anforderung der Kopplung der Daten umgesetzt werden kann. Wenn jedoch eine solche Kopplung ausbleibt, tragen die verarbeiteten Fingerabdruckdaten nicht wesentlich zur sicheren Identifikation bei. In diesem Falle stehen die mit der Verarbeitung der Fingerabdrücke verbundenen großen Gefährdungen insbesondere durch Missbrauch der Daten durch unberechtigte Nutzer und der geringe Nutzen der biometrischen Daten für eine sichere Identifikation in einem krassen Missverhältnis.

§ 16 Abs. 2 des Passgesetzes schreibt vor, dass Fingerabdrücke spätestens nach Aushändigung des Passes an den Passbewerber zu löschen sind. Damit ist auch eine längerfristige Speicherung in Datensicherungskopien unzulässig. Der Gesetzgeber hat mit dem sofortigen Löschgebot bewusst technische Schwierigkeiten in Kauf genommen, um die enge Zweckbindung sensibler Fingerabdruckdaten auch tatsächlich sicher zu stellen.

Die Löschungspflicht zum Zeitpunkt der Abholung umfasst sowohl das produktive System als auch den Datenbestand der Datensicherungen. Das Bundesinnenministerium und das Bundesamt für Sicherheit in der Informationstechnik (BSI) führen in ihrer „Handreichung Informationssicherheit für deutsche Passbehörden" dazu aus: „Für die temporären Informationen im Antragsverfahren – hier explizit die digitalen Fingerabdrücke – ist indes eine dauerhafte Speicherung unzulässig: Die Löschfristen müssen eingehalten werden und die Daten sind von der Datensicherung auszuschließen." Dieser Verpflichtung zur Löschung der Fingerabdruckdaten mit der Abholung des Passes wird das derzeitige Verfahren in Bezug auf die Backup-Dateien nicht gerecht.

Auch ein Jahr nachdem der HmbBfDI auf die Mängel hingewiesen und die Fachliche Leitstelle den Änderungsbedarf anerkannt hat, sind die Mängel immer noch nicht behoben. Derartige Zeitabläufe sind bei der Verarbeitung so sensibler Daten wie den Passantragsdaten aller Hamburgerinnen und Hamburger nicht akzeptabel, und die Mängel sind umgehend zu beheben.

18.2 Elektronischer Personalausweis (ePA)

Die Einführung des elektronischen Personalausweises bietet Chancen für das E-Government und den E-Commerce, doch offene Fragen müssen noch geklärt werden

Ab November 2010 wird der neue elektronische Personalausweis eingeführt. Während der bisherige Personalausweis nur optisch lesbar war, werden die Daten, einschließlich des biometrischen Gesichtsbildes, in Zukunft in einem in den Ausweis eingearbeiteten Funkchip gespeichert und elektronisch auslesbar sein. Der

ursprüngliche Plan, verpflichtend auch zwei Fingerabdrücke zu speichern, wurde, nicht zuletzt aufgrund der kritischen Stellungnahmen der Datenschutzbeauftragten und der Diskussion in der Öffentlichkeit, aufgegeben und in eine freiwillige Option geändert.

Die Nutzung des ePA zur Identifikation im Internet wird durch einen optionalen elektronischen Identitätsnachweis geschaffen, der es dem Inhaber ermöglicht, sich sowohl im E-Government als auch im E-Commerce gegenüber berechtigten Institutionen zu identifizieren oder, je nach Bedarf der angebotenen Dienstleistung, nur bestimmte Angaben, zum Beispiel zur Altersverifikation, zu übermitteln. Dabei ist der Besitz des ePA alleine zur Weitergabe der Daten nicht ausreichend. Vielmehr muss zusätzlich eine sechsstellige PIN eingegeben werden, was einen möglichen Missbrauch erschwert.

Der sogenannte Diensteanbieter muss, bevor er für den Empfang der Daten berechtigt wird, ein Berechtigungszertifikat beim Bundesverwaltungsamt beantragen. Dazu muss er nachweisen, zu welchem Zweck er welche Daten vom ePA des Kunden abrufen will. Dieses Verfahren führt einerseits dazu, dass der Diensteanbieter nur die Daten abfragen kann, die er tatsächlich braucht, und andererseits zu einer beiderseitigen Sicherheit, da sowohl der Ausweisinhaber (durch das im Internetangebot angegebene Berechtigungszertifikat) als auch der Dienstanbieter (bei Identifikation durch den ePA) weiß, mit wem er es zu tun hat. Diese Sicherheit ist bisher bei Internetgeschäften nicht gewährleistet. Dabei ist die Zusammenführung der Daten durch verschiedene Anbieter nicht möglich, da bei jeder Nutzung der digitalen Ausweisfunktion ein anderer Schlüssel erzeugt wird, der es dem Anbieter zwar ermöglicht, den Nutzer oder vielmehr den Ausweis wiederzuerkennen, der sich aber von dem bei einem anderen Anbieter erzeugten Schlüssel unterscheidet. Diese Regelungen sind sinnvoll und berücksichtigen datenschutzrechtliche Grundsätze. Sie können unserer Meinung nach allerdings auch dazu führen, dass dem Nutzer suggeriert wird, dass durch das Berechtigungszertifikat auch automatisch der sichere Umgang mit seinen Daten gewährleistet ist. Zwar soll der Diensteanbieter, im Rahmen einer Selbstverpflichtung, die Einhaltung von Datenschutz und Datensicherheit schriftlich bestätigen, doch das ist nicht ausreichend, um einen umfassenden Datenschutz zu gewährleisten. Die Möglichkeiten der missbräuchlichen Verwendung der Daten sind genauso gegeben wie beim bisherigen Ausweis. Daher ist es erforderlich, dass die Vergabe der Berechtigungszertifikate an die nachprüfbare Einhaltung von verbindlichen Datenschutzregelungen geknüpft und ihre Verletzung mit Sanktionsmöglichkeiten versehen wird.

Darüber hinaus wäre es zu begrüßen, wenn klare Regelungen geschaffen würden, die eventuelle Haftungsansprüche bei missbräuchlicher Nutzung regeln. Die gesetzliche Verpflichtung des Ausweisinhabers, den elektronischen Identitätsnachweis nur in einer sicheren Umgebung einzusetzen, wird alleine nicht ausreichen, in dieser Hinsicht Klarheit zu schaffen. Es ist nicht unwahrscheinlich, dass sich die technischen Sicherheitsmaßnahmen, die den Ausweisinhaber vor Identitätsdiebstahl und Missbrauch schützen sollen, im Laufe der 10jährigen Gültigkeit des ePA als nicht mehr ausreichend herausstellen könnten. Dieser Umstand, den der Gesetzgeber vorhersehen kann, darf nicht zu Lasten des Ausweisinhabers gehen.

IV. DATENSCHUTZ IM NICHT-ÖFFENTLICHEN BEREICH

1. Videoüberwachung

1.1 Videoüberwachung im öffentlichen Nahverkehr

Nachdem auch die HADAG Fähren mit Videoüberwachungstechnik ausgestattet worden sind, werden in Hamburg nun alle öffentlichen Verkehrsmittel videoüberwacht.

Die Erörterungen mit der HADAG über die Einführung von Videotechnik auf allen Fähren konnte im Berichtszeitraum abgeschlossen werden (vgl. 21. TB, 19.1). Auf den Fähren der HADAG wurden jeweils 2-4 Kameras im Fahrgastraum, 2 für die Rampen und 1 im Maschinenraum installiert. Die Kameras sind auf einen Monitor geschaltet, der sich im Schiffsführerstand befindet und von dem Schiffsführer beobachtet wird. Außerdem findet eine Aufzeichnung der Aufnahmen statt, die nach Ablauf von 24 Fahrzeugbetriebsstunden (48 Zeitstunden) automatisch überschrieben wird, wenn keine Auswertung erfolgt.

Gründe für den Einsatz von Videotechnik sind der zunehmende Vandalismus und vermehrte Diebstähle auf den Fähren sowie die Gewährleistung der Sicherheit der Fahrgäste beim Ein- und Ausstieg. Der Schiffsführer kann den Vorgang des Anlegens und Ablegens, bei dem hydraulische Rampen abgesenkt und angehoben werden, auf dem Monitor beobachten und so gefahrenträchtige Situationen frühzeitig erkennen. Die Überwachung des Maschinenraums geschieht aus technischen Gründen. Da die Fähren nur mit dem Schiffsführer als Besatzung fahren, soll der Schiffsführer durch eine Videoüberwachung des Maschinenraums frühzeitig z.B. Feuer- und Rauchentwicklung erkennen können. Die HADAG führte als Gründe für die Videoüberwachung eine Reihe von Vorfällen an, die sowohl gefährliche Ein- und Ausstiegssituationen als auch Vandalismus und weitere Straftaten betrafen.

Nach §6b BDSG ist Videoüberwachung 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. Wichtig dabei ist, dass allein das Motiv einer allgemeinen abstrakten Gefahrenvorsorge, etwa für den Schutz des Eigentums, nicht ausreicht. Vielmehr müssen belegbare Tatsachen die Annahme rechtfertigen, dass schwerwiegende Beeinträchtigungen drohen und es diese abzuwehren gilt. Solche belegbaren Tatsachen hat die HADAG vorgebracht. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hält die Argumentation der HADAG für nachvollziehbar

Es ist nicht ersichtlich, dass der durch die Videotechnik beabsichtigte Zweck – Sicherheit der Fährgäste, Verhinderung und Aufklärung von Diebstählen – auf andere Weise ebenso gut erreicht werden könnte. Zwar könnten die genannten Zwecke möglicherweise auch durch den Einsatz von mehr Personal auf den Fähren erreicht werden. Dies würde aber zu einem erheblichen finanziellen Mehraufwand und zu spürbaren Fahrpreiserhöhungen für die Kunden führen. Wir halten daher bei Abwägung der wirtschaftlichen und rechtlichen Interessen der HADAG mit den allgemeinen Persönlichkeitsrechten der Fahrgäste die Videoüberwachung auf den Fähren für vertretbar. Dabei war auch zu berücksichtigen, dass Maßnahmen zur Verhinderung eines Missbrauchs der Videoaufzeichnungen von der HADAG mit uns abgesprochen worden sind.

Beschwerden zur Videoüberwachung auf den HADAG Fähren liegen uns bisher nicht vor. Wir haben in den letzten Jahren auch keine Beschwerden zur Videoüberwachung in U-Bahnen, S-Bahnen und Bussen im Stadtgebiet erhalten. Dies mag daran liegen, dass die Bürger sich zunehmend an Videoüberwachung gewöhnen und diese unkritisch hinnehmen oder möglicherweise aufgrund mehrerer gravierender Vorfälle Videoüberwachung im öffentlichen Nahverkehr als unerlässlich für die eigene Sicherheit ansehen.

1.2 Videoüberwachung in Schwimmbädern

Die zunehmende Videoüberwachung in den Hamburger Schwimmbädern stößt auf datenschutzrechtliche Bedenken.

Bei einer im Jahr 2008 begonnenen Überprüfung stellten wir fest, dass in den Schwimmbädern der Bäderland GmbH zunehmend Videotechnik eingesetzt wird. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hält Videoüberwachung nach § 6b BDSG auch in Schwimmbädern aus Sicherheitsgründen in besonders gefahrträchtigen Bereichen (Rutschen) und zur Verhinderung sowie der Ermöglichung einer nachträglichen Aufklärung von Straftaten durch die Polizei in einem gewissen Rahmen für vertretbar. So wurde in der Vergangenheit mit der Bäderland GmbH abgesprochen, dass die in den Umkleiden befindlichen Schließfächer überwacht werden dürfen, wenn es ausreichend überwachungsfreie und als solche gekennzeichnete Umkleidemöglichkeiten für die Schwimmbadnutzer gibt. Auch eine auf besondere Wertschließfächer gerichtete Videokamera wurde als zulässig angesehen. Bei der Anbringung von weiteren Kameras ist jedoch zu berücksichtigen, dass die Nutzer eines Schwimmbads in der Regel ihre Freizeit dort verbringen und dabei nicht beobachtet werden wollen. Zur Verhinderung von Straftaten reichten daher nach unserer Auffassung in der überwiegenden Zahl der Fälle neben der auf die Schließfächer gerichteten Videokameras eine Überwachung des Eingangsbereichs des Schwimmbads und eine erhöhte Aufmerksamkeit des Personals aus.

Die Bäderland GmbH teilte diese Auffassung jedoch nicht uneingeschränkt. Insbesondere hinsichtlich einer auf ein Drehkreuz zur Sauna gerichteten Videokamera, die dazu dienen soll, ein unbefugtes Betreten durch Personen, die das Eintrittsgeld für die Sauna nicht bezahlt haben, zu verhindern, bestand Uneinigkeit. Bei einer Begehung vor Ort konnte festgestellt werden, dass dieser Zweck durch die angebrachte Kamera aus verschiedenen Gründen nicht erreicht werden kann und die Videoüberwachung daher ungeeignet ist. Die Verhinderung eines unbefugten Betretens des Saunabereichs kann durch andere Maßnahmen erreicht werden. Die Datenschutzaufsichtsbehörde kann auch nicht nachvollziehen, dass die Kamera am Drehkreuz zur Verhinderung von sexuellen Übergriffen in der Sauna erforderlich sein könnte, was von der Bäderland GmbH ebenfalls behauptet wird. Derartige Übergriffe können auch im Schwimmbad selbst erfolgen, wo keine Videokameras installiert sind. Sollte es aber tatsächlich einmal zu Vorfällen kommen, so wäre es möglich, die „Täter" anhand der Videobilder des Ein- und Ausgangsbereichs zu identifizieren. Mittlerweile hat die Bäderland GmbH die auf das Drehkreuz gerichtete Kamera abgebaut.

Nachgedacht wird von der Bäderland GmbH noch über die Anbringung weiterer Kameras im Bistrobereich eines Schwimmbads, in dem mehrfach nach Betriebsschluss Waren aus dem nicht abschließbaren Tresenbereich und aus abgeschlossenen Kühlschränken entwendet wurden. Wir halten diese Argumentation nicht für

ausreichend, die Erforderlichkeit von Videokameras zu begründen. Es gibt andere ebenso geeignete Maßnahmen, z.B. Einschließen der Waren im Tresenbereich und eine genaue Kontrolle des Kühlschrankinhalts und der ausgegebenen Schlüssel für die Kühlschränke, die zur Erreichung des beabsichtigten Zwecks ausreichen und weniger in die Betroffenenrechte eingreifen.

Insgesamt zeigt auch die Erörterung mit der Bäderland GmbH, dass Videoüberwachungstechnik von vielen Stellen als ein Allheilmittel angesehen wird und die verantwortlichen Stellen sich häufig gar nicht überlegen, ob es andere Möglichkeiten gibt, die beabsichtigten Zwecke zu erreichen. Dabei wird außer Acht gelassen, dass die ständige Präsenz von Kameras einen Überwachungsdruck erzeugen kann, der mit dem Risiko eines Autonomieverlustes der Betroffenen einhergeht. Auch wenn ein komplettes Verbot von Videoüberwachungskameras in vielen Bereichen nicht möglich sein dürfte, wird der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit in Einzelfällen genau prüfen, ob der Einsatz einzelner Videokameras den Voraussetzungen des § 6b BDSG entspricht.

1.3 Videoüberwachung in Einkaufszentren

Bei der Installation von Videoüberwachungstechnik in Einkaufszentren werden die gesetzlichen Anforderungen häufig nicht beachtet.

Durch eine Beschwerde wurden wir auf die umfassende Videoüberwachung in einem modernisierten Einkaufszentrum in Hamburg aufmerksam. Unsere Überprüfung ergab, dass die in Hamburg ansässige Betreibergesellschaft Videoüberwachungstechnik in dem größten Teil der von ihr im Hamburger Stadtgebiet und in anderen Bundesländern betriebenen Einkaufszentren installiert hat. Dabei wurden neben den Ein- und Ausgängen die Ladenstraßen, Eingänge zu einzelnen Geschäften, Rolltreppen, Gastronomie und Ruhebereiche, Kassenautomaten, Zugänge zu den Parkbereichen und die Parkdecks überwacht.

Nach § 6b BDSG ist eine Videoüberwachung öffentlich zugänglicher Räume zulässig, wenn sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interesse der Betroffenen überwiegen. Nach Angaben der Betreibergesellschaft erfolgt die Videoüberwachung in den Einkaufszentren zur Wahrnehmung des Hausrechts. Etwaige Vorkommnisse in der Ladenstraße sollen schnell erfasst werden, damit die Verwaltung schnell eingreifen könne. Zum Beispiel solle so verhindert werden, dass die Ladenstraße zum dauerhaften Aufenthalt oder Hausieren genutzt werden könne. Mit Hilfe der Videoüberwachung solle eine störungsfreie, angenehme Atmosphäre für die Kunden aufrechterhalten werden. Außerdem wird die Videoüberwachung nach Angaben der Betreibergesellschaft eingesetzt, um Straftaten generalpräventiv zu verhindern. Dies sei dann zulässig, wenn sich einschlägige Delikte mit einer gewissen Wahrscheinlichkeit ereignen würden, etwa weil es sich um geschäftstypische Straftaten handele, wie Ladendiebstähle in einem Kaufhaus. Im Jahr 2006/2007 habe es mindestens 35 Raubüberfälle, Einbrüche und Einbruchsversuche in den über 70 verwalteten Einkaufszentren gegeben. Außerdem hätten sich zahlreiche Diebstähle im Bereich der Ladenstraße ereignet, z.B. Taschendiebstahl und Diebstahl von Ausstellungsstücken von Mietern. Es sei zu Schlägereien und zu Sachbeschädigungen gekommen, BTM-Delikte hätten sich ereignet und Geldautomaten seien missbräuchlich genutzt worden.

Grundsätzlich ist eine Videoüberwachung zur Wahrnehmung des Hausrechts nach § 6b Abs. 1 Ziffer 1 BDSG zulässig. Das Hausrecht umfasst die Befugnis, Störer aus einem bestimmten Raum zu verweisen und ihnen das Betreten für die Zukunft zu untersagen. Bei der Prüfung im Hamburger Einkaufszentrum wurde jedoch festgestellt, dass eine Vielzahl von Kameras auf Bereiche gerichtet ist, in denen eine Störung des Hausrechts des Betreibers eher unwahrscheinlich ist, unter anderem in Gaststätten oder Eingängen zu einzelnen Geschäften. Zur Durchsetzung des Hausrechts des Betreibers sind diese Kameras nicht erforderlich. Die von der Betreibergesellschaft vorgebrachten Gründe für die umfassende Videoüberwachung betreffen jedoch nicht nur die Wahrnehmung des Hausrechts, sondern es geht insbesondere um die Verhinderung und Aufklärung von Straftaten in den Ladenstraßen.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat Zweifel, ob die Verhinderung und Aufklärung von Straftaten als berechtigtes Interesse der Betreibergesellschaft für die Videoüberwachung im Sinne des § 6b Abs. 1 Ziffer 3 BDSG angesehen werden kann. Dabei ist zu berücksichtigen, dass generalpräventive Maßnahmen und die Aufklärung von Straftaten in erster Linie öffentliche Aufgaben sind und dem Staat obliegen. Ein berechtigtes Interesse des Einzelnen oder von Unternehmen besteht regelmäßig nur im Schutz des eigenen Eigentums. Um den Schutz des Eigentums der Betreibergesellschaft geht es jedoch bei der Videoüberwachung ganz überwiegend nicht. Vielmehr dient die Überwachung in erster Linie dazu, Raubüberfälle, Diebstähle und Sachbeschädigungen bei Dritten (Ladeninhabern, Kunden) zu verhindern bzw. aufzuklären. Der Schutz des Eigentums Dritter vor Straftaten ist jedoch kein berechtigtes Interesse des Betreibers des Einkaufszentrums. Ebenso wie im öffentlichen Straßenraum ist es auch in Einkaufszentren Sache der Besucher, auf sich und ihr Eigentum aufzupassen. Eine etwaige Pflicht des Betreibers, für die Sicherheit seiner Besucher einzustehen, sehen wir nicht. Im öffentlich zugänglichen Raum besteht keine Berechtigung des einzelnen Bürgers oder von Unternehmen, überall dort, wo möglicherweise Straftaten vorkommen können, eine Videoüberwachung zu installieren. Die Verhinderung und Aufklärung von Straftaten gegenüber Dritten sowie von Belästigungen können wir daher nicht als berechtigtes Interesse des Betreibers an einer umfassenden Videoüberwachung in den Ladenstraßen anerkennen. Dabei ist auch zu berücksichtigen, dass mit der Begründung der abschreckenden Wirkung eine flächendeckende Überwachung der Einkaufsstraßen in den meisten Innenstädten möglich wäre.

Im Übrigen stehen die berechtigten Interessen der Kunden eines Einkaufszentrums einer umfassenden Videoüberwachung in den Ladenstraßen entgegen. Das Recht auf informationelle Selbstbestimmung schließt das Recht des Einzelnen ein, sich in der Öffentlichkeit frei bewegen zu können, ohne befürchten zu müssen, dass er ständig beobachtet wird. Die Schutzbedürftigkeit ist regelmäßig in öffentlichen Räumen hoch, in denen sich Menschen typischerweise länger aufhalten oder miteinander kommunizieren. Bei den Ladenstraßen in Einkaufszentren handelt es sich nicht um Durchgangsbereiche, die man rasch durchmisst. Einkaufszentren, in denen die Kunden wetterunabhängig ein breites Warenangebot vorfinden, wollen es den Kunden ermöglichen, zu verweilen und in Ruhe die Auslagen der Geschäfte anzusehen. Sitzgelegenheiten werden geschaffen und Gastronomie angesiedelt, um die Kunden zu binden und sie zu einem längeren Aufenthalt zu motivieren. Besucher, die dies tun, können sich der umfassenden und ständigen Videoüberwa-

chung jedoch nicht entziehen und werden dadurch in ihren Rechten unangemessen beeinträchtigt.

Im Berichtszeitraum wurde auch durch Datenschutzaufsichtsbehörden anderer Bundesländer die Videoüberwachung in von dem Hamburger Unternehmen betriebenen Einkaufszentren überprüft. Wegen der grundsätzlichen Bedeutung wurde über die Ergebnisse der Prüfungen und über den Umfang einer zulässigen Videoüberwachung in Einkaufszentren im Düsseldorfer Kreis, dem Gremium der Datenschutzaufsichtsbehörden, gesprochen. Ziel ist es, möglichst einheitliche Kriterien festzulegen, unter welchen Bedingungen eine Videoüberwachung in Einkaufszentren nach § 6b BDSG als zulässig angesehen werden kann. Über den Fortgang der Angelegenheit werden wir berichten.

1.4 Videoüberwachung in Restaurants

Die Inhaber von Gaststätten, Restaurants, Discos und anderen derartigen Unternehmen nutzen vielfach Videoüberwachung, um ihre Gäste zu kontrollieren. Dabei wird außer Acht gelassen, dass die Betroffenen das Recht haben, ihre Freizeit unbeobachtet zu genießen.

Bereits in den vorhergehenden Tätigkeitsberichten wurde über die zunehmende Videoüberwachung in verschiedenen Bereichen berichtet (vgl. z.B. 20.TB, 25., 21. TB, 19.). Im Berichtszeitraum sind in dieser Hinsicht weitere Branchen in den Fokus der Datenschutzaufsichtsbehörde geraten, was einerseits mit den deutlich gesunkenen Preisen derartiger Anlagen, andererseits auch mit der erhöhten Sensibilität und Aufmerksamkeit der Betroffenen zusammenhängt. Im Rahmen der einzelnen Prüfungen konnte festgestellt werden, dass bei den kontrollierten Unternehmen wenig Unrechtsbewusstsein vorhanden war, immer wieder auf vergleichbare Anlagen verwiesen wurde und bei vielen ein gewisser Gewöhnungseffekt hinsichtlich der mittlerweile vorausgesetzten Normalität von Überwachungen eintritt.

Dem entgegenzuwirken ist Aufgabe der Datenschutzaufsichtsbehörden. Nicht in allen Fällen wussten die betroffenen verantwortlichen Stellen überhaupt, dass für diese Art der Überwachung eine Rechtsgrundlage erforderlich ist. Andere wiederum legten die gesetzlichen Grundlagen sehr weit aus und berücksichtigten die schutzwürdigen Interessen der von der Überwachung Betroffenen nur sehr unzureichend.

Zunehmend haben die Datenschutzaufsichtsbehörde Beschwerden über Videoüberwachungen in Gaststätten, sogar in kleineren Cafés, aber auch in Unternehmen der Systemgastronomie erreicht. In erster Linie haben sich Gäste beschwert, die sich durch die Kameras in ihrer Privatsphäre gestört fühlen. Wir haben die betroffenen Unternehmen jeweils angeschrieben und Prüfungen vor folgendem Hintergrund vorgenommen:

Neben dem Risiko einer flächendeckenden Überwachung des Einzelnen durch öffentliche und private Stellen steht das Risiko eines Autonomieverlustes der betroffenen Gäste. Die ständige Präsenz von Kameras kann einen Überwachungsdruck erzeugen, der die Betroffenen verunsichern und in ihren Verhaltensalternativen einschränken kann. Die Vorschrift des § 6b BDSG soll diesen Gefahren einer ausufernden Videoüberwachung begegnen. Sofern öffentlich zugängliche Räume mit optisch-elektronischen Einrichtungen überwacht werden sollen, ist die Vorschrift zu beachten. Öffentlich zugängliche Räume sind alle diejenigen Bereiche, die von einem unbestimmten Personenkreis betreten werden können und von ihrer Zweck-

bestimmung her auch dazu bestimmt sind, von der Allgemeinheit betreten zu werden. Die Videoüberwachung ist nur in den gesetzlich geregelten Fällen unter Beachtung einer strikten Zweckbindung und Einhaltung des Erforderlichkeitsgrundsatzes möglich. In jedem Fall einer Videoüberwachung schreibt die gesetzliche Regelung eine umfassende Güter- und Interessenabwägung unter Beachtung der rechtlich geschützten Positionen sämtlicher Beteiligten unter Würdigung der Umstände des Einzelfalls vor.

Nach § 6 b BDSG ist eine Videoüberwachung nur zulässig, soweit sie aus den in der Vorschrift genannten Gründen erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Das ist im Bereich von Restaurationsbetrieben grundsätzlich nicht der Fall. Vielmehr ist die Schutzbedürftigkeit in solchen, als Rückzugsraum angesehenen, öffentlich zugänglichen Räumen als besonders hoch einzustufen. Dies trifft insbesondere auf die für die Kunden eingerichteten Sitzbereiche, die einen längeren und auch ungestörten Aufenthalt ermöglichen sollen, zu. Nur unter ganz besonderen Umständen, die im Einzelfall ausreichend begründet dargelegt werden müssen, kann es einmal zulässig sein, eine Videoüberwachung durchzuführen.

Ein Grund für die Zulässigkeit kann es sein, dass die Videoüberwachung zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Wichtig dabei ist, dass allein das Motiv einer allgemeinen abstrakten Gefahrenvorsorge, etwa für den Schutz des Eigentums, nicht ausreicht. Vielmehr müssen belegbare Tatsachen die Annahme rechtfertigen, dass schwerwiegende Beeinträchtigungen drohen, es diese abzuwehren gilt und Alternativen nicht zur Verfügung stehen.

Bei dieser Sachlage ist eine Videoüberwachung in der Regel in Gaststätten, Restaurants oder Cafés nicht erforderlich.

Darüber hinaus scheitert die Zulässigkeit auch daran, dass – angenommen, die Erforderlichkeit könnte ausnahmsweise vorliegen – schutzwürdige Interessen der Betroffenen jedenfalls überwiegen. Das Recht des Einzelnen, sich weitgehend überwachungsfrei im öffentlichen Raum bewegen zu können, ist ein Ausfluss des verfassungsrechtlich abgesicherten Rechts auf informationelle Selbstbestimmung. Niemand soll befürchten müssen, auf „Schritt und Tritt" beobachtet zu werden und gezwungenermaßen seine Verhaltensweise einer Dauerbeobachtung anzupassen. Gerade Restaurants, Bars, Eisdielen, Kneipen und sonstige Gaststätten dienen auch der Entspannung der Besucher, die sich nicht ständig dem Gefühl ausgesetzt sehen dürfen, dass ihr Verhalten beobachtet und sogar aufgezeichnet wird.

In einem Fall hatte ein Gast gegen die Videoüberwachung einer Kaffeehauskette gegen die Überwachung des Gastbereiches geklagt. In seinem Urteil zugunsten des Klägers führte das Amtgericht Hamburg (4 C 134/08) aus, dass das Recht auf informationelle Selbstbestimmung das Recht des Einzelnen verbürgt, sich in der Öffentlichkeit frei und ungezwungen bewegen zu dürfen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung gemacht zu werden.

Mit den Interessen der von der Videoüberwachung betroffenen Arbeitnehmer hat sich das Amtsgericht nicht auseinandersetzen müssen. Zu berücksichtigen ist in diesem Zusammenhang aber, dass auch Mitarbeiter der Unternehmen von der Videoüberwachung erfasst werden. Hinsichtlich der Überwachung von Arbeitnehmern ist ein besonders strenger Maßstab anzulegen und in der Regel ein überwiegendes schutzwürdiges Interesse der Mitarbeiter anzunehmen, das der Zulässig-

keit der Videoüberwachung entgegensteht. Dieser Punkt lässt sich auch nicht durch etwaige Vereinbarungen mit dem einzelnen Mitarbeiter oder eine Einwilligung überwinden, denn es wird in diesen Fällen im Arbeitsverhältnis in der Regel an der Freiwilligkeit mangeln.

Basierend auf der Rechtsprechung des Bundesarbeitsgerichts zur Videoüberwachung von Mitarbeitern ist daher in der Regel ein schutzwürdiges Interesse des Betroffenen anzunehmen. Ausnahmen sind nur unter ganz besonderen Voraussetzungen überhaupt möglich.

Videoüberwachung stellt einen erheblichen Eingriff in das allgemeine Persönlichkeitsrecht nicht nur der Gäste, sondern auch der betroffenen Arbeitnehmer dar. Das zulässige Maß einer Beschränkung des allgemeinen Persönlichkeitsrechts bestimmt sich nach dem Grundsatz der Verhältnismäßigkeit. Die Intensität einer Beeinträchtigung des allgemeinen Persönlichkeitsrechts hängt maßgeblich von der Dauer und der Art der Überwachungsmaßnahme ab. Gerade bei einer ständigen Überwachung kann sich der Arbeitnehmer dieser Maßnahme nicht entziehen, da er in der Regel den überwachten Bereich nicht verlassen kann. Die Intensität des Eingriffs in die Persönlichkeitsrechte der Arbeitnehmer ist deshalb als besonders hoch einzuschätzen.

Im Berichtszeitraum wurden auch mehrere Restaurants der sogenannten Systemgastronomie auf den Einsatz von Videoüberwachung geprüft. Problematisch war dabei, dass derartige Unternehmen Überwachungskonzepte entwickeln und unverändert in jedem Betrieb einsetzen. Gerade die Videoüberwachung erfordert jedoch eine Einzelfallbeurteilung, die die besonderen Gegebenheiten hinsichtlich der Lage und Gefährdung des Unternehmens in Abwägung mit den Individualinteressen der Gäste berücksichtigt. Angesichts der Vielzahl von Restaurationsunternehmen in Hamburg muss die Datenschutzaufsichtsbehörde ein hohes Maß an Überzeugungsarbeit leisten, um Veränderungen durchzusetzen. Bedauerlicherweise kann es hier nicht zu flächendeckenden Lösungen kommen.

1.5 Videoüberwachung und Wohnen

Grundeigentümer, Vermieter, aber auch Mieter installieren Überwachungskameras, nicht nur um Eigentumsübergriffe zu verhindern, sondern auch zur Kontrolle von Mitbewohnern.

In unserem letzten Tätigkeitsbericht (20. TB, 19.2) haben wir darauf hingewiesen, dass unsere Möglichkeiten im Falle von Überwachungen nicht öffentlicher Räumlichkeiten, wie etwa von Hausfluren oder Fahrstühlen in reinen Wohnhäusern beschränkt sind. Dies gilt jedoch nur für den Fall, dass keine Aufzeichnungen gefertigt werden. Im Falle der Anfertigung von Aufzeichnungen handelt es sich über die reine Beobachtung hinausgehend um eine Erhebung und Verarbeitung personenbezogener Daten, die auch bei nicht öffentlich zugänglichen Räumen nach der Vorschrift des § 28 Abs. 1 BDSG beurteilt werden kann. Ausgehend davon, dass genau solche Aufzeichnungen zunehmend erfolgen, haben sich im Bereich der Videoüberwachung von Wohnanlagen weitergehende Problembereiche entwickelt.

Immer wieder erreichen uns Beschwerden, die sich gegen Überwachungen öffentlicher Gehwege richten. Solche Anlagen werden von Hauseigentümern an Mehr- aber auch an Einfamilienhäuser angebracht, um entweder Straftaten gegen Fahrzeuge auf der Straße zu verhindern oder aufzuklären. Auch wenn man nicht den § 6 b BDSG heranzieht, der die Zulässigkeit nur für öffentlich zugängliche – private –

Räume beschreibt, sondern § 28 Abs. 1 BDSG, ist diese Art der Videoüberwachung unter keinem erdenklichen Gesichtspunkt zulässig. Im Rahmen des § 28 Abs. 1 BDSG ist nämlich in jedem Falle zwischen den berechtigten Interessen der verantwortlichen Stelle – in diesem Fall der jeweilige Eigentümer oder Verwalter – und den schutzwürdigen Interessen der Betroffenen eine Abwägung vorzunehmen. Selbstverständlich ist es anzuerkennen, dass Hausbewohner oder –eigentümer sich gegen Straftaten schützen und bereits begangene Straftaten einer Aufklärung zuführen möchten. Das kann jedoch nicht dazu führen, dass Passanten sich nicht mehr überwachungsfrei auf öffentlichen Gehwegen aufhalten können und immer damit rechnen müssen, von Videoüberwachungsanlagen erfasst zu werden. Private können in diesen Fällen nicht mehr Rechte für sich in Anspruch nehmen als die Polizei, die immer eine ausdrückliche Rechtsgrundlage haben muss. Das grundrechtlich geschützte informationelle Selbstbestimmungsrecht des Einzelnen gebietet es, derartige Aufzeichnungen, Beobachtungen und unkontrolliert mögliche Auswertungen von Bewegungen auf öffentlicher Straße zu verhindern.

Auch große Vermieter gehen dazu über, Hauseingänge, Treppenhäuser, Fahrstühle, Hausflure, Keller und Tiefgaragen per Video zu überwachen. Dabei wird oftmals nicht einmal abgewartet, ob überhaupt ein berechtigtes Interesse an einer solchen Maßnahme besteht, sondern sie wird schon vorsorglich ergriffen. In absoluten Ausnahmefällen kann dies möglich sein, wenn gravierende und belegbare Vorfälle in der Vergangenheit gerade in den konkreten Objekten gezeigt haben, dass es keine andere Lösung zum Schutze der Bewohner gibt. Unter solchen Einzelfallumständen müssen jedoch zur Wahrung der schutzwürdigen Interessen der Betroffenen, auch der Besucher, eine Reihe von flankierenden Maßnahmen getroffen werden, um die Datenschutzrechte zu wahren. Hierzu gehört unbedingt die Beteiligung eines betrieblichen Datenschutzbeauftragten, die Information aller Betroffenen und – ganz wichtig – ein Zugriffsschutz für die gefertigten Aufnahmen. Die Betroffenen müssen sich unter allen Umständen darauf verlassen können, dass die Aufnahmen nicht dazu benutzt werden können, ihre Lebensweise, ihr Kommen und Gehen auszuforschen. Dies lässt sich vor allem durch ein Blackboxverfahren erreichen, auf das niemand ohne konkreten Anlass Zugriff nehmen kann. Aber auch dies muss aus den bereits genannten Gründen als Ultima Ratio absoluten Ausnahmefällen vorbehalten bleiben.

In dem Bereich Videoüberwachung und Wohnen hat sich eine Neuerung ergeben, die datenschutzrechtlich als Besorgnis erregend anzusehen ist: Mittlerweile werden für hochwertigste Bauvorhaben Schutzkonzepte unter Einbeziehung von Videoüberwachung geplant, die davon ausgehen, dass die Bewohner ein erhöhtes Sicherheitsbedürfnis haben und derartige Vorkehrungen in ihrem direkten Wohnumfeld sogar erwarten. Solange die Überwachungsmaßnahmen keine öffentlichen Wege tangieren, die Bewohner den konkreten Maßnahmen freiwillig zustimmen (sie vielleicht sogar verlangen) und Besucher darauf hingewiesen werden, kann die Datenschutzaufsichtsbehörde dagegen nicht einschreiten. Gleichwohl ist auch diese Entwicklung als ein Schritt in Richtung auf eine immer engmaschiger werdende Videoüberwachung zu werten.

1.6 Beobachtung im Kino

Grundsätzlich ist die Beobachtung der Besucher eines Kinos während der Vorstellung nicht erlaubt. Eine Anfrage bei der Datenschutzaufsichtsbehörde betraf jedoch einen besonders zu beurteilenden Ausnahmefall.

Im Berichtszeitraum erreichte uns die Beschwerde eines Journalisten, der schilderte, dass bei der Pressevorstellung eines Films eine Überwachung mit Nachtsichtgeräten stattgefunden hatte. Die Aufklärung dieser Angelegenheit hat ergeben, dass die eingeladenen Journalisten bereits in der Einladung darauf hingewiesen wurden, dass die Filmvorführung zur Vermeidung unbefugter Aufzeichnungen überwacht wird. Der Film wurde vor dem offiziellen Kinostart ausschließlich geladenen Gästen vorgeführt. Darüber hinaus wurde noch einmal vor Betreten des Kinosaals deutlich auf die Beobachtung mit Nachtsichtgeräten hingewiesen. Eine Aufzeichnung fand nicht statt.

Unter diesen Umständen konnte nicht von einer Anwendbarkeit des Bundesdatenschutzgesetzes ausgegangen werden. Weder die Vorschrift über die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (§ 6b BDSG) noch diejenige über Datenerhebung, -verarbeitung und -nutzung (§28 BDSG) war hier einschlägig. Zum einen handelte es sich angesichts der Vorführung nur für geladene Gäste um eine geschlossene Veranstaltung und damit nicht um öffentlich zugängliche Räume, zum anderen wurde die Beobachtung nicht aufgezeichnet. Angesichts der für die Filmwirtschaft wichtigen Verhinderung von Raubkopien bereits vor dem Start eines begehrten Kinofilms kann dieses Ergebnis auch als sachgerecht angesehen werden. Vor dem offiziellen Kinostart ist auch davon auszugehen, dass die Pressevertreter keinen Anspruch darauf haben, die Vorstellung unbeobachtet zu besuchen und ihnen mit den vorher erteilten Informationen die Möglichkeit blieb, von dem Besuch abzusehen und auf den Beginn der normalen Vorstellungen zu warten.

Bei öffentlich zugänglichen Kinovorstellungen ist die Beobachtung der Kinobesucher mit Nachtsichtgeräten allerdings nach § 6b BDSG grundsätzlich unzulässig. Nachtsichtgeräte sind optisch-elektronische Einrichtungen, deren Einsatz nach § 6b I Nr. 3 BDSG zu beurteilen ist. Eine Einwilligung in die Überwachung durch bloßes Betreten eines Kinos scheitert jedenfalls am Merkmal der Freiwilligkeit. Zwar besteht ein berechtigtes Interesse der Filmverleiher, wirtschaftliche Einbußen durch sinkende Besucherzahlen und DVD-Verkäufe zu verhindern, doch sind die schutzwürdigen Interessen der betroffenen Personen an einem ungestörten Filmgenuss höher zu bewerten. Die Dunkelheit in Kinosälen vermittelt den Besuchern ein Gefühl der Privatheit und Intimität, was dazu führt, dass viele Menschen ihre Gefühle wie Trauer, Freude oder Angst offen zeigen sowie Zärtlichkeiten mit dem Partner/der Partnerin austauschen. Die Träger der Nachtsichtgeräte wählen den beobachteten Bereich selbständig aus, was ein erhebliches Missbrauchspotenzial eröffnet. Die Besucher können sich der Beobachtung nicht entziehen und werden, ohne dazu Anlass gegeben zu haben, unter Generalverdacht gestellt. Schließlich haben die aus dem militärischen Bereich stammenden Geräte eine nicht unerhebliche Einschüchterungswirkung.

Der Einsatz von Nachtsichtgeräten kann allerdings in absoluten Ausnahmefällen wie Vor- und Deutschlandpremieren zulässig sein. In diesen Fällen ist das wirtschaftliche Risiko der Filmverleiher besonders hoch, ebenso wie der Anreiz für Mitschneidende. Ist der Einsatz ausnahmsweise zulässig, muss dieser unter Hinweis auf die spezifische Art der Überwachung und die verantwortliche Stelle durch geeignete Maßnahmen bereits im Vorfeld der Vorführung angekündigt werden. Besucher, die der Überwachung entgehen wollen, können spätere Vorstellungen unbeobachtet besuchen.

2. Internationaler Datenverkehr

2.1 Übermittlung von Flugpassagierdaten nach Großbritannien

Zunehmend müssen sich die Datenschutzaufsichtsbehörden mit Datenanforderungen anderer Länder befassen, die nach deutschem Recht nicht zulässig wären.

Nachdem die Übermittlung von Flugpassagierdaten in die USA (vgl. 21.TB, 20.1) für viel Aufregung gesorgt hatte, fordern jetzt auch die britischen Zoll- und Sicherheitsbehörden von den Fluggesellschaften vor der Einreise der Passagiere die Übermittlung von Ausweisdaten. Abgesehen davon, dass Großbritannien von Deutschland aus mit dem herkömmlichen Personalausweis bereist werden kann, darf dieser nach § 4 Abs. 3 Personalausweisgesetz von den Fluggesellschaften weder zum automatischen Abruf personenbezogener Daten noch zur automatischen Speicherung personenbezogener Daten verwendet werden. Schon die automatisierte Erfassung dieser Daten ist daher nicht zulässig. Eine Rechtsgrundlage, die es erlauben würde, diese Daten an die britischen Zoll- und Sicherheitsbehörden zu übermitteln, ist ebenfalls nicht ersichtlich.

Die Schwierigkeit bei dieser nach Auffassung der Datenschutzaufsichtsbehörden unzulässigen Datenübermittlung besteht in der Tatsache, dass zwar die deutschen Fluggesellschaften deren Kontrolle nach dem Bundesdatenschutzgesetz unterliegen, Maßnahmen jedoch nur schwer getroffen werden können. Die Fluggesellschaften müssen sich, wenn sie ihre Passagiere dorthin befördern wollen, an die Vorgaben der britischen Zoll- und Sicherheitsbehörden halten. Jede Verfügung einer deutschen Aufsichtsbehörde, derartige Übermittlungen zu unterbinden, würde unweigerlich zu Problemen in der Beförderung von Passagieren nach Großbritannien führen.

Die Datenschutzaufsichtsbehörden haben daher im Rahmen des Düsseldorfer Kreises am 13. Juli 2009 zu diesem Thema einen Beschluss gefasst, der im Internet unter http://www.datenschutz-mv.de/dschutz/beschlue/eBorders.pdf abrufbar ist.

2.2 Mitarbeiterscreening durch international tätige Unternehmen

Internationale Konzerne schreiben ihren Mitgliedsunternehmen immer wieder Maßnahmen vor, die nach deutschem Recht nicht zulässig sind.

Durch die Anfrage einer norwegischen Kollegin wurde die Datenschutzaufsichtsbehörde auf ein Unternehmen in Hamburg aufmerksam, das von dem amerikanischen Mutterunternehmen zur Überprüfung seiner Mitarbeiter aufgefordert worden war, sich dem Global Restricted Party Screening anzuschließen. Ziel sollte es sein, auszuschließen, dass Beschäftigte Verbindungen zu Terrorismus, Drogengeschäften und anderem gesetzeswidrigem Verhalten haben. Die Listen von Personen, mit denen die Mitarbeiter abgeglichen werden sollten, werden von verschiedenen amerikanischen und internationalen Stellen geführt. Diese Listen enthalten nicht nur Einzelpersonen, sondern auch andere Unternehmen und Organisationen.

Datenschutzrechtlich stellt ein solcher Abgleich vor große Probleme. Nicht nur, dass Einträge in eine Reihe dieser Listen in das informationelle Selbstbestimmungsrecht der Betroffenen eingreifen; es sind auch gravierende existentielle Folgen bis hin zur Verweigerung von Sozialleistungen zu befürchten. Darüber hinaus sind diese Personen vielfach nicht eindeutig bezeichnet und es gibt so gut wie keine Möglichkeit, sich gegen die Aufnahme in eine solche Liste zu wehren und Rechts-

schutz geltend zu machen. Schon die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher im Jahre 2006 eine Entschließung gefasst und die Bundesregierung aufgefordert, bei den Vereinten Nationen und der Europäischen Union auf die Einhaltung der rechtsstaatlich gebotenen Standards zu dringen.

Es ist davon auszugehen, dass in Deutschland viele Tochtergesellschaften amerikanischer Unternehmen dazu aufgefordert werden, den beschriebenen Listenabgleich vorzunehmen. Hierfür gibt es jedoch keine Rechtsgrundlage nach dem Bundesdatenschutzgesetz, und auch eine Einwilligung der Mitarbeiter hätte mangels Freiwilligkeit keinen Bestand. Rechtlich zulässig ist ein Abgleich nur auf spezialgesetzlicher Grundlage gegen Listen, die die Anforderungen an die Berücksichtigung des informationellen Selbstbestimmungsrechts und der Rechtsstaatlichkeit des Zustandekommens aufweisen. Daher wurde der Düsseldorfer Kreis mit diesem Thema befasst, der im April 2009 einstimmig einen Beschluss gefasst hat, der im Internet unter http://www.datenschutz-mv.de/dschutz/ddk/Screening.html abrufbar ist.

3. Telekommunikation, Tele- und Mediendienste

3.1 Bewertungsportale

Das Internet bietet eine leicht zu handhabende Plattform, um sich über die Einschätzung von Personen zu informieren. Datenschutzrechte werden dabei häufig übersehen.

Immer wieder beschweren sich Betroffene über Beurteilungen ihrer Person in sogenannten Bewertungsportalen. Darunter versteht man Teledienste, die angeboten werden, um über das Internet Bewertungen oder Noten über Angehörige insbesondere von Berufsgruppen wie Professoren, Ärzte, Lehrer oder auch Handwerker abzugeben. Teilweise sind diese Bewertungen für jeden Internet-Nutzer lesbar, in wenigen Fällen ist eine vorherige Registrierung erforderlich. Ganz besonders einschneidend für die Betroffenen war die Möglichkeit, über eine amerikanische Seite Nachbarn zu beschimpfen. In diesen Fällen bestand für die Betroffenen keine Möglichkeit, sich schnell und wirksam zu wehren. Die Seite ist von Deutschland aus mittlerweile nicht mehr aufrufbar. Dies ist jedoch keine Gewähr dafür, dass nicht ähnliche Angebote wie etwa www.nachbarvz.de mit Sitz in Großbritannien auf den Markt drängen.

Datenschutzrechtlich gibt es viele Ansatzpunkte für eine kritische Beurteilung dieser Angebote. Nicht nur, dass diese Portale die Möglichkeit bieten, weitgehend anonym über jemanden, der namentlich genannt wird, seine persönliche Meinung zu sagen, auch die Tatsache, dass der Betroffene dagegen kaum etwas tun kann und den Urheber oft nicht kennt, führt zur Minimierung seiner Rechte. Eine Überprüfung des berechtigten Interesses der Nutzer findet – wie es z.B. bei Auskunfteien vorgeschrieben ist – nicht statt. Vielmehr kann jeder sich auf den meisten derartigen Portalen auch ohne irgendeinen Bezug zu der bewerteten Person über diese informieren. Im Rahmen des datenschutzrechtlich zur Verfügung stehenden Auskunftsrechts nach § 34 BDSG berufen sich die Anbieter in der Regel darauf, dass die Urheber von Bewertungen bei z.B. zusammengefasster Notengebung nicht mehr zu verifizieren sind. Im Übrigen unterlägen die Beiträge der freien Meinungsäußerung. Maßnahmen zur Qualitätssicherung der einzelnen Beiträge fehlen ebenso wie nach dem Datenschutzrecht vorgesehene Benachrichtigungen der Betroffenen.

Der Düsseldorfer Kreis der Datenschutzaufsichtsbehörden hat zu diesem Thema im April 2008 einstimmig einen Beschluss gefasst, der im Internet unter http://www.bfdi.bund.de/cae/servlet/contentblob/416828/publicationFile/25167/170408Internetportale.pdf abrufbar ist.

Ungeachtet dessen erging im Juni 2009 ein Urteil des Bundesgerichtshofes (IV ZR 196/08), das die Klage einer Lehrerin gegen die Bewertungsseite eines Schülerportals unter anderem mit der Begründung zurückgewiesen hat, dass das Recht der Meinungsfreiheit auch das Recht umfasst, mit seiner Meinung gehört zu werden und diese zu verbreiten. Es bestehe der Grundsatz des freien Meinungsaustauschs nicht nur für Themen, die von besonderem Belang für die Öffentlichkeit sind. Ob es in dieser Sache eine für die Belange des Datenschutzes positivere Entscheidung des Bundesverfassungsgerichts geben wird, bleibt abzuwarten.

Zum Schutz personenbezogener Daten ist zu bedenken, dass es auch unter Berücksichtigung der Meinungsfreiheit einen deutlichen Unterschied macht, ob eine Meinung mündlich, schriftlich oder auch in einer Schulzeitung geäußert wird oder ob sie nahezu frei über das Internet weltweit verbreitet wird.

3.2 Soziale Netzwerke

Soziale Netzwerke im Internet bieten einerseits eine an Verbreitungsgrad nicht zu überbietende Möglichkeit des Austauschs, andererseits sind damit vielfach nicht erkannte Gefahren für die informationelle Selbstbestimmung verbunden.

Besonders junge Leute nutzen in der heutigen Zeit häufig die sogenannten Sozialen Netzwerke im Internet, um Kontakt zueinander zu halten, alte Freunde wiederzufinden, neue Kontakte zu knüpfen, Meinungen auszutauschen, Antworten auf Fragen zu erhalten etc. Dabei handelt es sich um Internetplattformen der verschiedensten Art. In der Regel ist es erforderlich, dass die Nutzer sich anmelden und eigene Profile einstellen. Dies vermittelt oft den Eindruck, sich in einer durch andere nicht einsehbaren eigenen Welt zu befinden. Dabei wird verkannt, dass jeder sich anmelden kann, auch, um Informationen über andere Nutzer zu erhalten.

Die Datenschutzaufsichtsbehörden raten immer wieder zu ausgesprochen vorsichtigem Umgang mit den eigenen persönlichen Daten. Gleichwohl kommt es immer wieder vor, dass wir Beschwerden der unterschiedlichsten Art erhalten. Die einen geben freizügig unter ihrem richtigen Namen Dinge von sich preis, die sie sonst nur vertraulich an Freunde weitergeben, andere nehmen an Diskussionen mit Meinungen teil, die sie später bereuen. In beiden Fällen ist es möglich – und mit den Mitteln des Datenschutzes nicht zu verhindern, dass mit diesen Daten Missbrauch betrieben wird oder auch eine Kenntnisnahme Jahre später, z.B. bei einer Bewerbung, zu erheblichen Nachteilen führt.

Nicht immer können dafür die Betreiber der Sozialen Netzwerke verantwortlich gemacht werden. Diese sind allerdings gehalten, die rechtlichen Rahmenbedingungen des Angebots strikt zu beachten, um eine unter datenschutzrechtlichen Aspekten problemfreie Nutzung zu ermöglichen.

Der Düsseldorfer Kreis hat in seiner Sitzung im April 2008 einen Beschluss zur datenschutzkonformen Gestaltung sozialer Netzwerke verabschiedet, der im Internet unter http://www.bfdi.bund.de/cln_111/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/170408DatenschutzkonformeGestaltungSozNetzwerke.html?nn=409242 abrufbar ist.

Darüber hinaus hat sich auch die internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation mit dem Thema beschäftigt und einen Bericht und eine Empfehlung zum Datenschutz in sozialen Netzwerken, das „Rom Memorandum" verfasst (http://www.datenschutz-berlin.de/attachments/470/675.36.13.pdf?12348 67489).

Das Fraunhofer-Institut hat einzelne Soziale Netzwerke unter dem Gesichtspunkt Privatsphärenschutz in Soziale-Netzwerke-Plattformen untersucht und die Ergebnisse im September 2008 unter anderem unter http://www.sit.fraunhofer.de/Images/SocNetStudie_Deu_Final_tcm105-132111.pdf veröffentlicht. Die Kontrolle eines dort genannten Unternehmens durch die Datenschutzaufsichtsbehörde Hamburg hatte schon vor Kenntnis von der Studie begonnen und hat zu deutlichen Verbesserungen geführt.

Noch einmal muss aber betont werden, dass auch bei vollständig datenschutzgerechter Gestaltung der Angebote nicht die Gefahr ausgeschlossen werden kann, dass die Inhalte zweckfremd genutzt oder missbraucht werden. Jeder Nutzer muss hier besondere Vorsicht walten lassen und – soweit es das Angebot zulässt – auf die Angabe seines richtigen Namens verzichten.

Im Rahmen des Konzepts „Datenschutz 2010" werden wir genau diesen Ansatz verstärkt verfolgen und mit dem Projekt „Meine Daten kriegt ihr nicht!" besonders die Hamburger Schüler für das Thema sensibilisieren (mehr dazu vgl. unter I).

3.3 Google Street View

Die Fahrten der Google-Fahrzeuge zur Aufnahme von Straßenpanoramen haben in Deutschland für große Aufregung gesorgt. Intensive Verhandlungen mit dem Unternehmen führten zu deutlichen Verbesserungen für die von den Aufnahmen Betroffenen.

Seit Mitte 2008 erhielt die Aufsichtsbehörde Hamburg Hinweise darauf, dass Google mit Fahrzeugen in Deutschland Straßenpanoramen aufnimmt, um diese mit dem Produkt Google Street View ins Internet einzustellen. Viele der von den Aufnahmen Betroffenen sind über diese Entwicklung höchst besorgt. Betroffen ist nahezu jeder Bundesbürger, entweder als Fußgänger, Kfz-Besitzer oder auch als Bewohner oder Eigentümer einer der aufgenommenen Häuserfassaden.

Die Ansicht der Straßenpanoramen im Internet wird eine 360-Grad-Panoramadarstellung der aufgenommenen Straßen am Computer ermöglichen. Ziel des Unternehmens ist es, Deutschland möglichst flächendeckend zu erfassen. Andere Länder, wie z.B. Frankreich, Großbritannien und die USA können schon auf diese Weise im Internet betrachtet werden. Eine Veröffentlichung in Deutschland ist bisher noch nicht erfolgt, jedoch für die nächste Zeit beabsichtigt.

Die Befürchtungen zur Beeinträchtigung des Einzelnen durch die Veröffentlichung im Internet gehen verständlicherweise in verschiedene Richtungen. Es ist denkbar, dass einzelne Personen an Orten wiedererkannt werden, an denen sie nicht gesehen werden möchten oder sich in Situationen wiederfinden, die ihnen unangenehm sind. Dies gilt auch für die Erkennbarkeit von Kfz-Nummernschildern, die Rückschlüsse auf die Aufenthaltsorte von Fahrern oder Haltern zulassen. Besonders viele Betroffene haben sich auch an die Aufsichtsbehörde gewandt, um zu verhindern, dass Ansichten ihrer Wohnungen oder Häuser veröffentlicht werden. Dabei steht die Sorge im Vordergrund, dass Kriminelle örtliche Gegebenheiten zu Einbruchsversuchen auf einfache Weise am häuslichen Computer auskundschaften

könnten. Aber auch eine Beurteilung der wirtschaftlichen und sozialen Verhältnisse der Bewohner ist über diesen Weg nicht auszuschließen.

Angesichts der Tatsache, dass in diesem Fall ein amerikanisches Unternehmen Fahrzeuge mit hamburgischem Kennzeichen zur Erhebung der Aufnahmen einsetzt, musste zunächst die Anwendbarkeit deutschen Rechts und daran anschließend die örtliche Zuständigkeit geklärt werden. Im Ergebnis ließ sich feststellen, dass das deutsche Datenschutzrecht bei Erhebung der Daten im Inland anwendbar ist und das Unternehmen im Inland einen Vertreter zu benennen hat. Da die Google Germany GmbH, die zwar einen abweichenden Geschäftszweck hat, aber dem Konzern angehört, in Hamburg ansässig ist, hat Hamburg die Verhandlungen mit diesem inländischen Vertreter aufgenommen.

Datenschutzrechtlich ist die Problematik nicht ganz so einfach zu beurteilen, wie es auf den ersten Blick scheint. Die Datenschutzaufsichtsbehörden haben schon im November 2008 einen Beschluss zur datenschutzrechtlichen Bewertung von digitalen Straßenansichten insbesondere im Internet gefasst. Dieser kann unter http://www.bfdi.bund.de/cae/servlet/contentblob/416842/publicationFile/25165/141108DigitaleStrassenansichten.pdf abgerufen werden. Für den Kieler Landtag wurden zwei umfassende Gutachten erstellt, die unter http://www.landtag.ltsh.de/infothek/wahl16/umdrucke/3900/umdruck-16-3924.pdf und http://www.landtag.ltsh.de/infothek/wahl16/umdrucke/4400/umdruck-16-4418.pdf im Internet abrufbar sind. Diese Bewertungen konnten im Laufe der Gespräche mit dem Unternehmen im Jahre 2009 angesichts zunehmender Erkenntnisse über die genaue Ausgestaltung des beabsichtigten Angebots in konkrete Forderungen einfließen.

Nach den Vorschriften des Bundesdatenschutzgesetzes ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn die Daten allgemein zugänglich sind, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt. Daraus ergibt sich angesichts der Tatsache, dass die Aufnahmen ausschließlich auf öffentlichen Straßen gefertigt werden und damit allgemein zugänglich sind, die Notwendigkeit einer genauen Abwägung zwischen den Interessen des Unternehmens und den schutzwürdigen Interessen der Betroffenen. Ein offensichtliches Überwiegen aller Betroffeneninteressen konnte nicht von vornherein angenommen werden, weil das Produkt durchaus auch eine Vielzahl von Befürwortern hat. Die Datenschutzaufsichtsbehörde Hamburg stand also vor der schwierigen Aufgabe, in Verhandlungen mit dem Unternehmen ein Ergebnis zu erzielen, das den schutzwürdigen Interessen aller Betroffenen gerecht wird.

Ein erster Durchbruch konnte im Vorfeld der Sitzung des Düsseldorfer Kreises im April 2009 erreicht werden. Neben den sowieso von Google vorgesehenen Verpixelungen der Gesichter und Kfz-Kennzeichen hat das Unternehmen zugestanden, für Deutschland eine Widerspruchsmöglichkeit zu schaffen, die es Eigentümern und Mietern ermöglicht, gegen die Darstellung von Häuserfassaden schon vor, aber auch nach Veröffentlichung Widerspruch einzulegen. Darüber hinaus wurde zugesichert, die jeweils aktuell befahrenen Gebiete auf der Seite von Google zu veröffentlichen. Bedauerlicherweise gab es während mehrerer Monate hinsichtlich der Veröffentlichung der aufzuzeichnenden Orte erhebliche Probleme. Auch wurde erst im Mai bekannt, dass die Gesichter und Kfz-Kennzeichen und damit auch die Häuserfassaden, gegen deren Veröffentlichung Widerspruch eingelegt wird, un-

verändert in den bei Google in den USA befindlichen Rohdaten erhalten bleiben sollten. Gleichzeitig fehlten hinsichtlich der Zusagen noch schriftliche Bestätigungen des amerikanischen Unternehmens. Sogar eine Videokonferenz Anfang Juni 2009 mit Unternehmensvertretern in den USA und der Schweiz brachte nicht sofort den erhofften Durchbruch in diesen Fragen. Erst weitere schwierige Verhandlungen bis Ende Juni 2009 führten dazu, dass Google die Zusage gab, auch die Rohdaten der Widersprechenden unkenntlich zu machen. Vor dem Hintergrund der im Folgenden aufgelisteten konkreten Zusagen sind die Betroffenenrechte angemessen berücksichtigt:

1. Google hat verbindlich zugesichert, eine Technologie zur Verschleierung von Gesichtern vor der Veröffentlichung von derartigen Aufnahmen einzusetzen.
2. Google hat verbindlich zugesichert, eine Technologie zur Verschleierung von Kfz-Kennzeichen vor der Veröffentlichung derartiger Aufnahmen einzusetzen.
3. Google hat verbindlich zugesichert, Widerspruchsmöglichkeiten zur Entfernung bzw. Unkenntlichmachung eines Gebäudes durch einen Bewohner oder Eigentümer vorzuhalten und derartige Widersprüche zu bearbeiten.
4. Google hat verbindlich zugesichert, dass Widersprüche zu Personen, Kennzeichen und Gebäuden bzw. Grundstücken bereits vor der Veröffentlichung von Bildern in einer einfachen Form berücksichtigt werden mit der Folge, dass die entsprechenden Bilder vor der Veröffentlichung unkenntlich gemacht werden. Voraussetzung ist eine Identifizierung des Grundstücks, der Person oder des Fahrzeugs.
5. Google hat verbindlich zugesichert, die geplanten Befahrungen mit einem Hinweis auf die Widerspruchsmöglichkeit im Internet rechtzeitig vorher bekannt zu geben. Die vorhandenen Befahrungspläne werden bis zu zwei Monate im Voraus veröffentlicht und ständig aktualisiert. Google hat die verbindliche Zusage gemacht, die Liste genauer zu gestalten und auf Landkreise und kreisfreie Städte zu erstrecken. Dies wurde zwischenzeitlich umgesetzt.
6. Google hat verbindlich zugesagt, dass die Widerspruchsmöglichkeit auch nach der Veröffentlichung noch besteht.
7. Die Rohdaten werden nach Aussage von Google zum Zwecke der Weiterentwicklung und Verbesserung der von Google entwickelten Technologie zur Unkenntlichmachung von Gesichtern, Kfz-Kennzeichen und Gebäudeansichten benötigt. Google hat verbindlich zugesichert, die Löschung/Unkenntlichmachung der Rohdaten vorzunehmen, indem die Ergebnisse aus dem Prozess zur Unkenntlichmachung von Gesichtern und Kfz-Kennzeichen in die Rohdaten übernommen werden, sobald die Speicherung und Verarbeitung der Rohdaten nicht mehr für die genannten Zwecke erforderlich ist.
8. Google hat verbindlich zugesichert, die Löschung oder Unkenntlichmachung der Rohdaten von Personen, Kfz und Gebäudeansichten vorzunehmen, die aufgrund eines Widerspruchs zu entfernen sind. Die Löschung oder Unkenntlichmachung dieser Daten in den Rohdaten wird bereits vor der Veröffentlichung vorgenommen, wenn der Widerspruch bis zu einem Monat vor Veröffentlichung der Bilder bei Google eingeht. Später oder auch nach Veröffentlichung eingehende Widersprüche führen zu einer Löschung in den Rohdaten binnen zwei Monaten.
9. Google hat die Erstellung eines Verfahrensverzeichnisses zugesichert.

10. Im Falle von Verknüpfungen des Dienstes durch andere Anbieter behält sich Google in den Nutzungsbedingungen das Recht vor, bei offensichtlicher Verletzung anwendbarer Gesetze, die Schnittstelle zu unterbinden.
11. Google hat zugesichert, eine Beschreibung der Datenverarbeitungsprozesse und der technischen und organisatorischen Maßnahmen für Google Street View vorzulegen. Insbesondere gehört hierzu auch eine deutliche Beschreibung des Umgangs mit den Widersprechendendaten von der Entgegennahme des Widerspruchs bis zur endgültigen Löschung bzw. Unkenntlichmachung.
12. Widerspruch kann eingelegt werden im Internet unter http://maps.google.de/intl/de/help/maps/streetview/faq.html#q7 oder schriftlich bei der Google Germany GmbH, betr.: Street View, ABC-Straße 19, 20354 Hamburg. Der Link mit dem Text: „FAQ Street View (inkl. Widerspruchsmöglichkeiten)" ist nunmehr direkt auf der ersten Seite der Hilfeseiten für Google Maps Deutschland erreichbar. Diese Hilfeseiten erreicht jeder Nutzer direkt aus dem Produkt Google Maps Deutschland, wenn er oben rechts den Link „Hilfe" klickt.
13. Die bei Google eingelegten Widersprüche werden zeitnah bestätigt. E-Mails mit Widersprüchen werden bereits bestätigt, alle entsprechenden Briefe werden fortlaufend beantwortet.

Die Kontrolle der Datenschutzaufsichtsbehörde ist damit jedoch keineswegs abgeschlossen. Vielmehr stehen wir weiterhin in engem Kontakt mit dem Unternehmen und beobachten sehr genau die Einhaltung der Zusagen. Dieser Prozess wird sich noch einige Zeit hinziehen, zumal die Veröffentlichung noch nicht erfolgt ist und ein Termin zur Veröffentlichung auch noch nicht feststeht.

Neben den Schwierigkeiten des Unternehmens, die zu befahrenden Orte zu veröffentlichen, haben Informationen aus der Schweiz, in der es für einige Gebiete schon eine Internetpräsenz gibt, zu neuen Gesprächen über die Wirksamkeit der Verpixelungen geführt. Zu Irritationen kam es hierbei auch durch eine wissenschaftliche Veröffentlichung von Google selbst, in der die erfolgreiche Verpixelung von Gesichtern in lediglich 90% aller Fälle festgestellt wird (geringfügig besser für Kfz-Kennzeichen mit ca. 95%). Dies würde bedeuten, dass jedes zehnte auf einem Street-View-Bild abgebildete Gesicht erkennbar bliebe. Wir sind daraufhin in direkten Kontakt mit den Autoren und zuständigen Ingenieuren bei Google getreten und haben die ergänzende Information erhalten, dass die Rate unerkennbarer Gesichter bei den veröffentlichten Street-View-Bildern tatsächlich bei 98% liegen wird, da neben Verpixelung weitere Aspekte zur Unkenntlichkeit beitragen, etwa Größe, Entfernung, Lichtverhältnisse. Ob dies eingehalten wird, bleibt abzuwarten. Hierbei ist auch die weitere Entwicklung der Diskussion in der Schweiz von Interesse, da die Verpixelungsqualität einen der vom Eidgenössischen Datenschutzbeauftragten bemängelten und gerichtlich zu klärenden Aspekte darstellt.

Im weiteren Verlauf ist damit zu rechnen, dass die Möglichkeit, vorab Widerspruch gegen die Veröffentlichung von Häusern, Kfz- und Personenabbildungen einzulegen, von Google erhebliche organisatorische und verfahrenstechnische Vorkehrungen verlangt. Wir werden diesen Prozess durch geeignete Maßnahmen begleiten und die Einhaltung der gemachten Zusagen überwachen.

Die Erhebung von Geodaten zum Zweck der späteren Nutzung kann in weiten Bereichen personenbezogene Daten betreffen. Insoweit fallen Projekte wie Google Street View in den Schutzbereich des Bundesdatenschutzgesetzes. Deren Durchführung erfordert zur Sicherung des informationellen Selbstbestimmungsrechts Betroffener zahlreiche Vorkehrungen, die als Ergebnis von komplexen Abwägungs-

und Planungsentscheidungen möglichst frühzeitig von der Daten erhebenden Stelle garantiert werden sollten. Hierzu zählen die Anonymisierung und die Einräumung von Verfahrensrechten Betroffener, denen es bereits vorab möglich sein muss, der Abbildung ihrer Person, ihrer Häuser und Grundstücke sowie ihrer Kfz zu widersprechen. Die nachträgliche Beachtung der Anonymisierungsanforderungen durch die verantwortliche Stelle muss zudem bereits bei der Erhebung der Daten sichergestellt sein und die verantwortliche Stelle muss zusichern, nach Veröffentlichung der Bilder die Rohdaten unkenntlich zu machen.

Insgesamt ist festzuhalten, dass sich die Generalklauseln des Bundesdatenschutzgesetzes für die Beurteilung von Projekten zur Erhebung von Geodaten als wenig taugliche Regulierungsgrundlage erweisen. Eine spezialgesetzliche Normierung der Erhebung und Nutzung von Geodaten würde einen einheitlichen und rechtssicheren Rahmen gerade für private Anbieter bereitstellen. Hierfür sprechen die große wirtschaftliche Bedeutung derartiger Datensammlungen sowie die vielfältigen Konflikte mit den Persönlichkeitsrechten Betroffener, die sich aus der Sammlung von Geodaten und der jederzeitig möglichen globalen Abrufbarkeit über das Internet zwangsläufig ergeben.

Die zu diesem Thema veröffentlichten Presseerklärungen und die Zusagen können unter http://www.hamburg.de/datenschutz/ nachgelesen werden.

3.4 Google Analytics und andere Trackingsysteme

Web-Tracking muss den datenschutzrechtlichen Anforderungen genügen.

Unternehmen haben ein Interesse zu erfahren, in welchem Umfang ihre Webseiten genutzt werden. Dienstleister bieten dafür Tools an, mit denen solche Analysen durchgeführt werden können. Dabei sind die datenschutzrechtlichen Vorgaben des Telemediengesetzes (TMG) zu beachten. Der Düsseldorfer Kreis hat dazu in seiner Sitzung im November 2009 folgenden Beschluss gefasst:

Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten

Viele Web-Seitenbetreiber analysieren zu Zwecken der Werbung und Marktforschung oder bedarfsgerechten Gestaltung ihres Angebotes das Surf-Verhalten der Nutzerinnen und Nutzer. Zur Erstellung derartiger Nutzungsprofile verwenden sie vielfach Software bzw. Dienste, die von Dritten kostenlos oder gegen Entgelt angeboten werden.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass bei Erstellung von Nutzungsprofilen durch Web-Seitenbetreiber die Bestimmungen des Telemediengesetzes (TMG) zu beachten sind. Demnach dürfen Nutzungsprofile nur bei Verwendung von Pseudonymen erstellt werden. Die IP-Adresse ist kein Pseudonym im Sinne des Telemediengesetzes.

Im Einzelnen sind folgende Vorgaben aus dem TMG zu beachten:

- Den Betroffenen ist eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen. Derartige Widersprüche sind wirksam umzusetzen.
- Die pseudonymisierten Nutzungsdaten dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Sie müssen gelöscht werden, wenn ihre Speicherung für die Erstellung der Nutzungsanalyse nicht mehr erforderlich ist oder der Nutzer dies verlangt.
- Auf die Erstellung von pseudonymen Nutzungsprofilen und die Möglichkeit zum Widerspruch müssen die Anbieter in deutlicher Form im Rahmen der Datenschutzerklärung auf ihrer Internetseite hinweisen.

- Personenbezogene Daten eines Nutzers dürfen ohne Einwilligung nur erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Jede darüber hinausgehende Nutzung bedarf der Einwilligung der Betroffenen.
- Die Analyse des Nutzungsverhaltens unter Verwendung vollständiger IP-Adressen (einschließlich einer Geolokalisierung) ist aufgrund der Personenbeziehbarkeit dieser Daten daher nur mit bewusster, eindeutiger Einwilligung zulässig. Liegt eine solche Einwilligung nicht vor, ist die IP-Adresse vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist.

Werden pseudonyme Nutzungsprofile durch einen Auftragnehmer erstellt, sind darüber hinaus die Vorgaben des Bundesdatenschutzgesetzes zur Auftragsdatenverarbeitung durch die Anbieter einzuhalten.

Ein Produkt zur Webanalyse bietet Google mit Google Analytics an. Bereits im Jahr 2006 haben wir gegenüber Google dargelegt, dass Google Analytics nicht den datenschutzrechtlichen Anforderungen genügt. Google nahm das Produkt seinerzeit aus anderen Gründen vom Markt. Nachdem im Jahr 2008 das Tool wieder angeboten wurde, hatten wir die Gespräche mit Google erneut aufgenommen, um ein den datenschutzrechtlichen Anforderungen des § 15 Abs. 3 TMG entsprechendes Produkt zu erreichen. Festzustellen ist, dass die im Beschluss des Düsseldorfer Kreises genannten Vorgaben derzeit von Google nicht erfüllt werden. Der Einsatz von Google Analytics ist daher unzulässig. Gleiches gilt für entsprechende Trackingsysteme anderer Dienstleister.

Wir haben Google über den Beschluss des Düsseldorfer Kreises informiert.

Webseitenbetreiber, die ein nicht den Anforderungen entsprechendes Tool einsetzen, handeln ordnungswidrig und müssen mit der Einleitung eines Bußgeldverfahrens rechnen.

3.5 Bildergalerien über Partys im Internet

Bevor Fotos ins Internet gestellt werden, müssen sich die Verantwortlichen über die rechtlichen Grundlagen informieren.

Im Berichtszeitraum erreichten uns mehrere Beschwerden über im Internet veröffentlichte Fotos. Dies waren solche, die von Privaten, aber auch z.B. von Vereinen oder Fotografen ins Internet gestellt worden waren.

Hochzeiten, Abiturfeiern und andere gesellschaftliche Ereignisse jeder Art werden häufig von anwesenden Fotografen begleitet. Deren Geschäft besteht darin, die gefertigten Aufnahmen anschließend zur Erinnerung an die Aufgenommenen zu verkaufen. Früher mussten diese sich in der Regel an das Fotostudio wenden, um Bilder zu bestellen oder wurden von den Veranstaltern damit bedacht. In letzter Zeit ist es üblich geworden, die Aufnahmen zur Bestellung ins Internet zu stellen und so zu gewährleisten, dass jeder sich in Ruhe zuhause entscheiden kann.

Nicht bedacht wird bei dieser Form der Vermarktung, dass jedem Einzelnen der aufgenommenen Personen ein Recht am eigenen Bild zusteht und angesichts der weltweiten Zugänglichkeit insbesondere die erhebliche Gefahr der Fertigung von Kopien und Verwendung für Zwecke aller Art besteht. Rechtlich muss für jede derartige Veröffentlichung – mit Ausnahme von Bildnissen der Zeitgeschichte, von solchen, auf denen die Personen nur Beiwerk darstellen und wenigen anderen Fällen – eine Einwilligung jedes Betroffenen vorliegen. Das bedeutet, dass die Teilnehmer

von Veranstaltungen, bei denen fotografiert wird, zumindest deutlich darauf aufmerksam gemacht werden müssen, dass die Bilder ins Internet gestellt werden. Sie müssen außerdem jederzeit die Möglichkeit haben, einer solchen Vorgehensweise für die von ihnen gefertigten Aufnahmen zu widersprechen. Ein Widerspruch nach der Veröffentlichung muss unverzüglich zur Entfernung der Bilder im Internet führen. Um die Persönlichkeitsrechte auch derjenigen, die mit der Veröffentlichung angesichts der mittlerweile eingetretenen Üblichkeit dieser Verfahrensweise einverstanden sind, zu gewährleisten, sind die Fotos passwortgeschützt einzustellen. Das bedeutet für Fotografen auf Veranstaltungen, dass sie dort bekannt geben müssen, mit welchem Passwort die Bilder auf ihrer Seite aufgerufen und bestellt werden können.

Aber nicht nur für Fotografen, sondern auch für andere gilt mit wenigen Ausnahmen, dass sie sich vor Veröffentlichung von Fotos mit einzelnen erkennbaren Personen deren Einverständnis einholen müssen.

4. Versicherungswirtschaft

4.1 Einwilligungs- und Schweigepflicht-Entbindungserklärung

Trotz intensiver Erörterungen mit der Versicherungswirtschaft konnte bisher keine Einigung auf eine neue Formulierung für eine Einwilligungs- und Schweigepflicht-Entbindungserklärung erzielt werden.

Der vom Gesamtverband der Versicherungswirtschaft (GDV) vorgelegte Entwurf einer Einwilligungs- und Schweigepflicht-Entbindungserklärung gilt für die Verarbeitung von Gesundheitsdaten durch Versicherungen. Die Erklärung berücksichtigt zum einen die Anforderungen des § 213 Versicherungsvertragsgesetzes (VVG) für die Erhebung von personenbezogenen Gesundheitsdaten (vgl. 21. TB, 22.1). Zum anderen ist die Abgabe der Erklärung durch den Versicherungsnehmer bzw. Antragsteller auch für die weitere Verarbeitung von Gesundheitsdaten erforderlich, da § 28 Abs. 7 BDSG als Rechtsgrundlage nach überwiegender Meinung der Datenschutzaufsichtsbehörden nicht für private Versicherungen gilt. In dem vorliegenden Entwurf wird den Betroffenen die Möglichkeit eröffnet, eine Schweigepflicht-Entbindungserklärung für eine eventuelle Prüfung der Leistungspflicht des Versicherers bereits bei Abschluss des Vertrags oder erst später in jedem Leistungsfall abzugeben. In jedem Fall muss der Betroffene vor der Datenerhebung unterrichtet und auf sein Widerspruchsrecht hingewiesen werden.

Wir sind der Auffassung, dass der derzeit vorliegende Entwurf noch nicht den datenschutzrechtlichen Anforderungen entspricht. In der Arbeitsgruppe Versicherungswirtschaft bestand Konsens darüber, dass die Schweigepflicht-Entbindungserklärung nur bei solchen Versicherungen zum Einsatz kommen dürfe, bei denen die Erhebung von Gesundheitsdaten relevant sei und dass diese Sparten ausdrücklich in der Überschrift benannt werden müssten. Dies ist bisher nicht erfolgt. Vielmehr ist den allgemeinen Hinweisen zu der Erklärung zu entnehmen, dass die Schweigepflicht-Entbindungserklärung auch in Versicherungssparten genutzt werden soll, in denen von vornherein nicht vermutet wird, dass Gesundheitsdaten verarbeitet werden müssen, z.B. in der Reisegepäckversicherung und Kfz-Versicherung. Eine Beschränkung des Einsatzes der Schweigepflicht-Entbindungserklärung auf bestimmte Sparten ist bisher nicht erkennbar. Dies ist mit den Vorschriften des BDSG nicht vereinbar.

Personenbezogene Daten dürfen nur erhoben werden, wenn sie für die Durchführung des Vertrags erforderlich sind. Die Erhebung von Gesundheitsdaten bei Antragstellung ist erforderlich bei Kranken-, Lebens-, Berufsunfähigkeitsversicherungen usw. Nur in diesen Fällen muss bei Antragstellung eine Schweigepflicht-Entbindungserklärung abgegeben werden und darf eine entsprechende Erklärung in den Versicherungsantrag aufgenommen werden. Dies gilt nicht für die in den Hinweisen genannte Reisegepäckversicherung oder Kfz-Versicherung. Es mag in Ausnahmefällen bei der Schadensabwicklung im Rahmen derartiger Versicherungsverträge erforderlich sein, Gesundheitsdaten zu verarbeiten. Wenn dies so ist, muss im Einzelfall nachträglich von den Versicherungsunternehmen gefordert werden, dass die Betroffenen eine Schweigepflicht-Entbindungserklärung abgeben. Es ist nicht zulässig, in allen Versicherungssparten, in denen eine Verarbeitung von Gesundheitsdaten im Rahmen der Vertragsabwicklung theoretisch notwendig werden kann, auf Vorrat die Abgabe einer Schweigepflicht-Entbindungserklärung zu fordern. Eine ausdrückliche Klarstellung, wann die Klausel eingesetzt werden soll, ist daher erforderlich. Weitere Bedenken richten sich gegen den fehlerhaften Hinweis auf die Datenverarbeitung im Hinweis- und Informationssystem (HIS) der Versicherungswirtschaft. Dieses System wird derzeit nicht von den Krankenversicherungen genutzt. Ob weitere in der Erklärung genannte Punkte auch für die Verarbeitung von Daten bei Krankenversicherungen relevant sind (z.B. Übermittlung von Gesundheitsdaten an Rückversicherer) muss noch geklärt werden.

Insgesamt zeigt der Entwurf der Schweigepflicht-Entbindungserklärung, dass der Versuch, eine Erklärung zu formulieren, die für alle Versicherungen in Frage kommt, häufig mit einem Verlust an Transparenz und Verständlichkeit für die Betroffenen einhergeht.

4.2 Verhaltensregeln

Die Mehrheit der Datenschutzaufsichtsbehörden hält den bisher von der Versicherungswirtschaft vorgelegten Entwurf für Verhaltensregeln nach § 38a BDSG noch nicht für datenschutzkonform.

Der Gesamtverband der Versicherungswirtschaft (GDV) hat im Berichtszeitraum einen Entwurf für Verhaltensregeln vorgelegt, die für die Versicherungswirtschaft einheitliche Standards zur Gewährleistung und Förderung der Durchführung von datenschutzrechtlichen Regelungen schaffen sollen. Vor dem Hintergrund der mehrjährigen Diskussion mit den Datenschutzaufsichtsbehörden hatte der mit dem Entwurf durch den GDV beauftragte ehemalige Berliner Datenschutzbeauftragte vorgeschlagen, als notwendige Inhalte die Punkte Warn- und Hinweissystem, Datenerhebung bei Vorversicherern, Datenübermittlungen bei Rückversicherern, Auftragsdatenverarbeitung und Funktionsübertragung, Datenverwendung durch Vermittler, Berater und Betreuer sowie Bonitätsabfragen und Scoring in die Verhaltensregeln aufzunehmen. Wesentliche Bedeutung sollte der Präzisierung der Abwägungsklauseln des BDSG im Hinblick auf die versicherungsspezifischen Datenverarbeitungsprozesse zukommen.

Ein erster Entwurf der Verhaltensregeln wurde vom GDV im Dezember 2007 vorgelegt. Dieser sowie die in der Folgezeit gefertigten Änderungsentwürfe wurden im Kreis der Datenschutzaufsichtsbehörden in der AG Versicherungswirtschaft sehr kontrovers diskutiert. Ein Versuch, die Verhaltensregeln in der Frühjahrssitzung 2009 des Düsseldorfer Kreises zu verabschieden, scheiterte daran, dass 11 Daten-

schutzaufsichtsbehörden den vorgelegten Entwurf für nicht abstimmungsreif hielten gegen 4 befürwortende und 2 enthaltende Stimmen.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit gehört zu den Datenschutzaufsichtsbehörden, die den Entwurf der Verhaltensregeln sehr kritisch beurteilen. Nach § 38 a BDSG dienen Verhaltensregeln der Durchführung von datenschutzrechtlichen Regelungen. Die Verhaltensregeln sollen die aus dem Datenschutzrecht resultierenden Handlungs- und Unterlassungspflichten auf eine branchen- und praxisnahe Weise konkretisieren und präzisieren, so dass sie von den Verbandsmitgliedern auch gut umgesetzt werden können (siehe Bizer in Simitis, Kommentar zum Bundesdatenschutzgesetz, 5. Aufl., § 38 a BDSG, Rdnr. 42 ff.). Nach der genannten Kommentierung sind Beispiele für Verhaltensregeln die Auslegung einzelner Erlaubnistatbestände, nach denen personenbezogene Daten verarbeitet werden dürfen, die anwendungsbezogene Konkretisierung unbestimmter Rechtsbegriffe und die Präzisierung von Abwägungsklauseln durch Fallgruppen. Auch stärkere Garantien als sie im staatlichen Datenschutzrecht vorgesehen sind, können in Verhaltensregeln vorgesehen werden. Es bestehen erhebliche Zweifel, dass der vom GDV vorgelegte Entwurf für Verhaltensregeln diesen Anforderungen gerecht wird. Der Entwurf gibt in weiten Teilen die geltende Gesetzeslage wieder und enthält vorwiegend allgemeine Grundsätze ohne die für Verhaltensregeln notwendigen Konkretisierungen, Präzisierungen, Beispielsfälle und Fallgruppen. Insbesondere die einzelnen Regelungen zu den oben aufgezählten notwendigen Punkten enthalten nur eine Wiedergabe der in §§ 28 und 29 BDSG enthaltenen allgemeinen Abwägungsklausel.

Die Verhaltensregeln enthalten in den strittigen Fragen zwar keinen Minuswert, sie enthalten aber auch keinen Mehrwert, der geeignet wäre, die jahrelangen Diskussionen zu beenden. So weisen beispielsweise die Regelungen zu Bonitätsauskünften, zum Scoring, zum Hinweis- und Informationssystem, zur Werbung und Markt- und Meinungsforschung sowie zum Datenaustausch mit Vorversicherern und Rückversicherern nur auf eine noch vorzunehmende Interessenabwägung zwischen den berechtigten Interessen der Versicherungen und den schutzwürdigen Interessen der Betroffen ohne Lösungsansätze hin. Daher wird die Diskussion zwischen Datenschutzaufsichtsbehörden und der Versicherungswirtschaft zu den meisten der oben genannten zentralen Probleme auch bei Vorliegen der Verhaltensregeln fortgeführt werden müssen. Ein Nutzen der Verhaltensregeln im Hinblick auf die seit Jahren streitigen Fragestellungen wird daher nicht gesehen.

Insgesamt erscheinen die bisher vorliegenden Verhaltensregeln nicht geeignet, die Durchführung datenschutzrechtlicher Bestimmungen in der Versicherungsbranche tatsächlich zu fördern.

4.3 Warn- und Hinweissystem

Die Versicherungswirtschaft wird bis 2011 die Struktur des Auskunftverfahrens im Rahmen des Warn- und Hinweissystems ändern und das System ab diesem Zeitpunkt in Form einer Auskunftei nach § 29 BDSG betreiben.

Der Austausch personenbezogener Daten im Rahmen des Warn- und Hinweissystems (HIS) wird seit Jahren in der Arbeitsgruppe Versicherungswirtschaft mit den Vertretern des Gesamtverbands der Versicherungswirtschaft (GDV) diskutiert. Die Datenschutzaufsichtsbehörden hatten massive Kritik an dem bisherigen Verfahren geäußert (siehe zuletzt 21. TB, 22.3) und der Versicherungswirtschaft eine Frist bis

zum 1. Januar 2009 für die Umsetzung eines neuen Konzepts für das System gesetzt.

Der GDV hat den Datenschutzaufsichtsbehörden im Berichtszeitraum die neue Struktur des HIS vorgestellt. Das Warn- und Hinweissystem soll in Form einer Auskunftei nach § 29 BDSG wahrscheinlich nicht vom GDV selbst sondern von einer noch zu beauftragenden Auskunftei betrieben werden. Die Versicherungsunternehmen sind über den Umbau des Systems und den Stand der Arbeiten unterrichtet, so dass sie die notwendigen Schritte für die Implementierung in die Unternehmenssysteme planen können. Nach Angaben des GDV wird wegen der Komplexität des Systems, der damit verbundenen technischen Veränderungen und dem Implementierungsbedarf bei den Versicherungsunternehmen die Umsetzung erst im Jahre 2011 abgeschlossen werden können. In der Übergangszeit bis 2011 wird der GDV den Betroffenen auf Anfrage Auskünfte darüber erteilen, ob und mit welchen Daten sie in HIS gemeldet sind. Dies war bisher nicht erfolgt, da der GDV in der bisherigen Struktur des HIS als Auftragsdatenverarbeiter handelt. Auskünfte an die Betroffenen wurden daher auf Anfrage nur durch die einmeldenden Versicherungsunternehmen erteilt.

Angesichts der jahrelangen Verhandlungen wurde die Verzögerung bis zur endgültigen Systemumstellung durch die Datenschutzaufsichtsbehörden massiv kritisiert. Der GDV hat den Datenschutzaufsichtsbehörden neben der zentralen Auskunftserteilung an die Betroffenen angeboten, dass auch eine Benachrichtigung der einzumeldenden natürlichen Personen durch die einzelnen Versicherungsunternehmen erfolgen soll. Diese Übergangslösung, die für Transparenz bei den Betroffenen sorgt und ihnen die Geltendmachung ihrer Rechte auf Auskunft, Berichtigung und Löschung von Daten ermöglicht, wurde von den Datenschutzaufsichtsbehörden grundsätzlich akzeptiert. Sie erklärten sich bereit, Ordnungswidrigkeitenverfahren wegen der strukturellen Defizite des HIS gegen Versicherungsunternehmen jedenfalls dann nicht einzuleiten, wenn eine entsprechende Benachrichtigung durch die Unternehmen erfolgt.

Über die inhaltliche Ausgestaltung des HIS und die Einmeldegründe wird derzeit intensiv in einer Arbeitsgruppe mit Vertretern der Datenschutzaufsichtsbehörden und des GDV diskutiert. Die Neukonzeption des HIS sieht weiterhin eine Spartentrennung bei der Auskunftserteilung vor. Es wird eine Differenzierung zwischen Antrags- und Leistungsprüfung und den dafür einzumeldenden Daten vorgenommen. Die Kommunikation über das neue HIS soll ausschließlich elektronisch erfolgen. Die über das HIS übermittelten Daten sollen nicht alleinige Entscheidungsgrundlage für die Versicherungsunternehmen sein, sondern nur Hinweise geben, die bei der Leistungsprüfung mit einer Detailauskunft durch Anfrage bei den einmeldenden Versicherungsunternehmen konkretisiert werden können. Detailauskünfte im Antragsbereich werden dagegen wegen kartellrechtlicher Vorgaben nicht mehr erteilt werden. Wegen dieser Beschränkungen im Antragsbereich beabsichtigt der GDV, den Katalog der einzumeldenden Daten durch die Versicherungsunternehmen deutlich zu erhöhen. So wird zum Beispiel in der Lebensversicherung angedacht, sämtliche Ärzte, die von den Versicherungsnehmern im Antrag angegeben werden, einzumelden. Durch eine solche Liste soll ein Abgleich der Angaben ermöglicht werden, falls ein Antragsteller bei mehreren Unternehmen einen Antrag stellt.

Die Datenschutzaufsichtsbehörden haben erhebliche Zweifel an der rechtlichen Zulässigkeit der Einmeldung von am Versicherungsverhältnis nicht beteiligten Drit-

ten wie Ärzten in HIS. Zum Teil wird die Auffassung vertreten, dass es sich bei der Angabe von Ärzten um besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG handelt, was erhöhte Anforderungen an die Zulässigkeit der Datenverarbeitung bedeuten würde. Außerdem wird davon ausgegangen, dass schutzwürdige Interessen der Ärzte der Einmeldung entgegen stehen.

Auch der Absicht des GDV, künftig jede BU-Rente ab einer Rentenhöhe von 9000 Euro jährlich einzumelden, stehen die Datenschutzaufsichtsbehörden sehr kritisch gegenüber. Da eine BU-Rente von 9000 Euro jährlich der Regelfall sein wird, entstünde auf diese Weise eine private Datei über den größten Teil der in Deutschland abgeschlossenen BU-Renten. Bisher ist jedoch vom GDV nicht nachvollziehbar dargelegt worden, dass ein so umfassender Datenbestand zur Missbrauchsbekämpfung erforderlich sein könnte.

Positiv sehen die Datenschutzaufsichtsbehörden dagegen die Änderung der Meldekriterien im Bereich Rechtsschutz. Eine Einmeldung in HIS erfolgt nur noch bei vier oder mehr Schadensfällen in den vergangenen zwölf Monaten.

Während der weiteren Gespräche wird darauf zu achten sein, dass die Versicherungswirtschaft die Umstrukturierung des HIS nicht zu einer aus Sicht des Datenschutzes ungerechtfertigten Erweiterung des Datenbestandes nutzt.

5. Auskunfteien

5.1 Neuregelungen im Bundesdatenschutzgesetz

Die Neuregelungen im Bundesdatenschutzgesetz wirken sich nicht nur indirekt auf den Bereich der Auskunfteien aus. Die entsprechenden Vorschriften wurden auch direkt erweitert und verändert.

Bisher wurde als Rechtsgrundlage für die Übermittlung personenbezogener Daten durch Unternehmen an Auskunfteien die allgemeine Rechtsgrundlage des § 28 BDSG herangezogen. Am 1. April 2010 tritt nun mit § 28a BDSG auch eine Vorschrift in Kraft, die speziell die Datenübermittlung an Auskunfteien betrifft. Unternehmen dürfen dann nur noch auf der Grundlage dieses Gesetzes personenbezogene Daten an Auskunfteien melden. Bereits vor Jahren (19. TB, 21.1) wurde darüber berichtet, dass die Datenschutzaufsichtsbehörden Maßstäbe dafür entwickelt hatten, unter welchen Umständen Unternehmen bei offenen Forderungen Übermittlungen an Auskunfteien vornehmen dürfen. Diese Maßstäbe wurden vor dem Hintergrund festgelegt, dass Betroffeneninteressen angemessen zu berücksichtigen sind. Angesichts immer wieder bekannt gewordener Verstöße gegen diese Einschränkungen werden jetzt ähnliche Voraussetzungen ausdrücklich ins Gesetz aufgenommen. Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien darf ab Inkrafttreten des Gesetzes nur noch unter den dort aufgeführten Umständen stattfinden. Mit Absatz 2 des neuen § 28a BDSG wird künftig auch geregelt werden, unter welchen Umständen Kreditinstitute personenbezogene Daten über Vertragsverhältnisse an Auskunfteien übermitteln dürfen. Hierüber ist der Betroffene auch vor Vertragsabschluss zu unterrichten. In der Vergangenheit hat es immer wieder Differenzen zwischen den Datenschutzaufsichtsbehörden und der Kreditwirtschaft über die Zulässigkeit der Meldung von Giroverträgen ohne Überziehungsmöglichkeit gegeben. Mit dem neuen § 28a Abs. 2 BDSG wird die Meldung derartiger Verträge ebenso ausgeschlossen wie die Meldung von vorvertraglichen Verhandlungen, die den Betroffenen dazu dienen, Konditionen zu ermitteln. Um zu verhindern, dass die Unternehmen es versäumen, Än-

derungen zu gemeldeten Daten auch an die Auskunfteien zu übermitteln, wird darüber hinaus vorgeschrieben, dass die Änderungen innerhalb eines Monats nach Kenntniserlangung auch der Auskunftei mitzuteilen sind. Ein Verstoß gegen diese Verpflichtung wird als Ordnungswidrigkeit nach § 43 Abs. 1 Nr. 4a BDSG geahndet werden können. Die Auskunftei wiederum muss das Unternehmen über die Löschung unterrichten.

Die Datenschutzaufsichtsbehörden haben zwar die Voraussetzungen, die das Gesetz jetzt regelt, im Wesentlichen schon unter Geltung der alten Gesetzeslage aufgestellt. Da dies jedoch einer Abwägung folgte, werden durch die Regelung Diskussionen mit Auskunfteien und Unternehmen künftig reduziert. Die Datenschutzaufsichtsbehörden werden die Umsetzung kritisch begleiten.

Es wird auch zu beobachten sein, welche Auswirkungen die künftige Regelung des § 28b BDSG zum Scoring auf die Übermittlung von Scorewerten durch Auskunfteien haben werden. Auch Auskunfteien ermitteln Scorewerte und geben diese im Rahmen von Anfragen zu Betroffenen an Unternehmen weiter. Zwar bezieht sich die Vorschrift nicht direkt auf Auskunfteien, jedoch auf deren Kunden. Insofern werden die Auskunfteien ebenso wie die Unternehmen selbst die Vorgaben des § 28b BDSG zu beachten haben, weil anderenfalls ihre Kunden gegen datenschutzrechtliche Vorschriften verstoßen. Zu den Einzelheiten des § 28b BDSG vgl. unter IV 6.1.

Die in § 29 BDSG geregelte Tätigkeit der Auskunfteien selbst wurde vor dem Hintergrund der neuen §§ 28a und 28b BDSG angepasst. Darüber hinaus gelten ab dem 11. Juni 2010 neue Vorschriften, die sich aus dem Gesetz zur Umsetzung der Verbraucherkreditrichtlinie ergeben.

5.2 Auskünfte an die Wohnungswirtschaft

Noch immer sperren sich die Vertreter der Auskunfteien, speziell auf die Wohnungswirtschaft zugeschnittene Auskünfte an die Wohnungswirtschaft zu erteilen.

Obwohl bereits seit Jahren in der Arbeitsgruppe Auskunfteien des Düsseldorfer Kreises eine Einigung mit den Vertretern der Wohnungswirtschaft hinsichtlich der Auskünfte an Vermieter angestrebt wird, konnte noch immer kein tragfähiges und allgemein gültiges Ergebnis erzielt werden. Zuletzt wurde im 21. Tätigkeitsbericht (24.3) ausführlich dargelegt, unter welchen Voraussetzungen die Datenschutzaufsichtsbehörde in Hamburg eine Auskunft an Vermieter für zulässig bzw. unzulässig hält.

Im Berichtszeitraum wurde noch einmal der Versuch unternommen, von den Auskunfteien eine Zusage dahingehend zu erhalten, dass Auskünfte an anfragende Vermieter nur noch unter Berücksichtigung konkreter Vorgaben erfolgen. Da eine entsprechende Einigung gescheitert ist, hat sich der Düsseldorfer Kreis erneut mit der Angelegenheit befasst und im Oktober 2009 einen Beschluss gefasst. Daraus geht hervor, unter welchen eingeschränkten Umständen Bonitätsauskünfte über Mietinteressenten eingeholt werden dürfen. Der Beschluss kann unter http://www.datenschutz-mv.de/dschutz/beschlue/Bonitausk.pdf im Internet nachgelesen werden.

Die Datenschutzaufsichtsbehörden werden den Beschluss den Auskunfteien und Vermietern zur Kenntnis geben und bekannt werdende Verstöße ahnden.

6. Kreditwirtschaft

6.1 Transparenz bei Scoring-Verfahren

Künftig müssen Kreditinstitute auf Anfrage Betroffenen Auskunft über das Zustandekommen und die Bedeutung eines Scorewertes in allgemein verständlicher Form erteilen.

Die Datenschutzaufsichtsbehörden haben in der Vergangenheit gegenüber der Kreditwirtschaft immer wieder gefordert, dass Scoring-Bewertungen für die Betroffenen transparent sein müssen (vgl. 21. TB Ziffer 25.1) Nach Auffassung der Datenschutzaufsichtsbehörden ergab sich dieses Informationserfordernis vor der Novellierung des BDSG aus der Abwägung der berechtigten Interessen der Kreditinstitute mit den schutzwürdigen Interessen der Betroffenen gemäß § 28 Abs. 1 Nr. 2 BDSG. Für die Betroffenen müsse nachvollziehbar sein, welche personenbezogenen Merkmale in die Berechnung des Score-Wertes einfließen, welche konkreten personenbezogenen Daten der Kredit suchenden Person dafür genutzt wurden und welches die maßgeblichen Merkmale sind, die den konkreten Score-Wert der betroffenen Person negativ beeinflusst haben. Diese maßgeblichen Merkmale sollen nach dem Grad ihres Einflusses auf den konkreten Score-Wert aufgelistet werden. Die Forderungen wurden von der Kreditwirtschaft regelmäßig nicht erfüllt.

In einer Beschwerde gegen ein in Hamburg ansässiges Kreditinstitut rügte der Betroffene, dass ihm keine Auskunft über die Kriterien des Kreditscorings gegeben wurde. Der Beschwerdeführer hatte von dem Kreditinstitut ein Werbeschreiben mit einem Kreditangebot ab 3,9 % erhalten. Er übersandte den ausgefüllten Antrag mit Angaben zu seinem Nettoeinkommen (ca. 3500 Euro), seiner Miete (350 Euro) und weiteren monatlichen Kreditbelastungen (ca. 800 Euro) an das Kreditinstitut, das ihm daraufhin ein neues Kreditangebot mit einem Zins von 7,9 % unterbreitete. Auf seine Forderung, ihm Auskunft über die Kriterien der Entscheidung zu erteilen, verwies das Kreditinstitut auf sein Geschäftsgeheimnis und verweigerte die Auskunft über die Einzelheiten des Kreditscorings. Der Beschwerdeführer fühlte sich durch das Kreditinstitut getäuscht und vertrat die Auffassung, dass sich das Unternehmen auf diesem Weg personenbezogene Daten der Antragsteller verschaffen wollte. Außerdem hatte er den Verdacht, dass seine Wohnanschrift in den neuen Bundesländern trotz seiner grundsätzlich guten Bonitätsdaten zu einer Erhöhung des Zinses für das Kreditangebot geführt hatte.

Leider war es uns wegen der zu diesem Zeitpunkt geltenden Gesetzeslage nicht möglich, die Forderung nach mehr Transparenz mit Hilfe der Vorschriften des BDSG durchzusetzen. Die Regelung des Auskunftsanspruchs in § 34 BDSG ließ mehrere Auslegungsmöglichkeiten zu und die Nichterteilung einer Auskunft war nach § 43 BDSG nicht mit einem Bußgeld bewehrt.

Durch Einführung des § 29b BDSG mit Wirkung ab 1. September 2009 hat der Gesetzgeber nun Voraussetzungen für die Erhebung und Verwendung eines Wahrscheinlichkeitswerts (Score-Werts) für ein bestimmtes zukünftiges Verhalten des Betroffenen festgelegt. Nach § 34 Abs. 2 ist dem Betroffenen bei dem Einsatz von Scoring-Verfahren künftig auf Verlangen Auskunft über die Wahrscheinlichkeitswerte, die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten sowie das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemeinverständlicher Form zu erteilen. Wird eine Auskunft nach § 34 Abs. 2 nicht, nicht richtig, nicht vollständig oder nicht

rechtzeitig erteilt, können die Datenschutzaufsichtsbehörden nach § 43 Abs. 1 Ziffer 8a BDSG künftig Bußgelder von bis zu 50.000 Euro verhängen.

Die Neuregelungen sind Folge der von Daten- und Verbraucherschützern seit langem geübten Kritik an der Intransparenz von Scoring-Verfahren. Scoring-Verfahren werden nicht nur in der Kreditwirtschaft, sondern insbesondere auch durch Auskunfteien und in weiten Teilen des Versandhandels eingesetzt. Derzeit ist noch nicht absehbar, wie die Unternehmen die neuen Regelungen umsetzen werden. Es wird davon ausgegangen, dass in der Arbeitsgruppe Kreditwirtschaft, in der Datenschutzaufsichtsbehörden mit Vertretern der Kreditwirtschaft Themen von grundsätzlicher Bedeutung ansprechen, die Ausgestaltung der Auskünfte über Scoring-Verfahren durch Kreditinstitute intensiv erörtert werden wird. Wir werden darüber berichten.

6.2 Unzulässige Datenerhebung durch Kreditinstitut

Wegen der unzulässigen Erhebung von personenbezogenen Daten für institutsinterne Qualitätssicherungsmaßnahmen wurde ein Bußgeld in Höhe von 7500 Euro verhängt.

Im Berichtszeitraum erhielten wir eine Beschwerde von zwei Rechtsanwälten, die sich gegen die Einholung einer Bonitätsauskunft bei einer Handelsauskunftei durch ein Hamburger Kreditinstitut richtete. Das Kreditinstitut hatte eine Bonitätsauskunft über die Rechtsanwälte mit dem Anfragegrund „Kreditentscheidung" eingeholt. Die Rechtsanwälte standen jedoch zum Zeitpunkt der Anfrage in keinerlei Geschäftsverbindung zu dem Kreditinstitut. Sie hatten dort weder einen Kredit beantragt noch unterhielten sie ein Konto.

Das Kreditinstitut räumte ein, dass kein berechtigtes Interesse im Sinne des § 29 Abs. 2 Nr. 1a BDSG zur Erhebung von Daten über die Rechtsanwälte vorlag. Hintergrund der Anfrage sei eine Maßnahme zur Qualitätssicherung im Bereich der Bonitätsentwicklung gewesen. Das Kreditinstitut habe überprüfen wollen, wie aussagekräftig die Bonitätseinschätzung der Handelsauskunftei im Verhältnis zu den dem Kreditinstitut selbst vorliegenden Bonitätsentwicklungen bei vielen Rechtsanwälten und Rechtsanwaltskanzleien sei, mit denen das Kreditinstitut Verträge habe. Auf der Internetseite www.rechtsanwalt.com/hamburg/ gäbe es eine Übersicht über die in Hamburg tätigen Rechtsanwälte. Man habe Anfragen über die in der Übersicht befindlichen Rechtsanwälte, die Kunden des Kreditinstituts gewesen seien, bei der Handelsauskunftei getätigt. Die Beschwerdeführer hätten sich auf der Liste „zwischen" mehreren Kunden des Kreditinstituts befunden, so dass irrtümlich auch zu ihnen eine Bonitätsauskunft eingeholt worden sei.

Die Erhebung von Daten über die Beschwerdeführer stellte eine Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 1 BDSG dar. Das Kreditinstitut hat fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhoben.

Die Bonitätsauskunft enthielt personenbezogene Daten über die Rechtsanwälte. Neben dem Geburtsdatum und der Privatanschrift der beiden Rechtanwälte enthielt die Auskunft Angaben über die berufliche Betätigung, die Zahl ihrer Mitarbeiter, die Aktiva und Verbindlichkeiten sowie die Zahlungsweise im Zusammenhang mit ihrer Tätigkeit und einen Bonitätsindex, der zur schnellen Beurteilung der Zahlungsfähigkeit des Geschäftspartners dient. Bei diesen Informationen handelt es sich um Einzelangaben über persönliche und sachliche Verhältnisse von Personen gemäß § 3 Abs. 1 BDSG.

Diese Daten sind nicht allgemein zugänglich. Handelsauskunfteien verarbeiten Daten, die nur zum Teil aus öffentlichen Registern oder Registern mit besonderen Zugangsvoraussetzungen wie dem Schuldnerverzeichnis stammen. Daneben erhalten sie Informationen durch Vertragspartner, z.B. über deren Erfahrungen mit der Zahlungsweise ihrer Kunden. Die Handelsauskunftei wertet zudem statistische Informationen aus und errechnet einen sogenannten Bonitätsindex, der eine Prognose zur Beurteilung der Zahlungsfähigkeit einer Person abgibt und auf einer Vielzahl von Kennwerten (z. B. Eigenkapital, Liquidität, Erlös, Zahlungsverhalten) basiert. Eine Auskunft enthält daher grundsätzlich eine Vielzahl von Daten, die nicht allgemein zugänglich sind. Dies war auch bei der Auskunft über die Beschwerdeführer der Fall.

Die Datenerhebung durch das Kreditinstitut war unbefugt. Die Erhebung von Bonitätsdaten bei einer Handelsauskunftei durch ein Kreditinstitut ist nur zulässig, wenn die Kenntnis der Daten zu vertraglichen Zwecken für die Beurteilung der Kreditwürdigkeit der Betroffenen unmittelbar relevant oder aus anderen Gründen zur Wahrung berechtigter Interessen des Kreditinstituts erforderlich ist (§ 28 Abs. 1 Satz 1 Nr. 1 und 2 BDSG). Ein solches Interesse bestand nicht, da es zwischen dem Kreditinstitut und den Rechtsanwälten keine Vertragsbeziehung gab. Eine Beurteilung der Bonität der Rechtsanwälte durch das Kreditinstitut war daher nicht erforderlich.

Die unbefugte Datenerhebung war zumindest fahrlässig erfolgt, da die in Angelegenheiten des Datenschutzes erforderliche verkehrsübliche Sorgfalt durch das Kreditinstitut nicht beachtet worden ist. Das Kreditinstitut hat sich vor Erhebung der Daten nicht vergewissert, dass es sich bei den Rechtsanwälten tatsächlich um ihre Vertragspartner handelte. Allerdings wäre die Anfrage bei der Auskunftei auch dann unter keinem erdenklichen Gesichtspunkt zulässig gewesen, wenn die Rechtsanwälte Kunden des Kreditinstituts gewesen wären. Derartige Maßnahmen zur Qualitätssicherung im Bereich der Bonitätsentwicklung bei Rechtsanwälten sind mit den Vorschriften des BDSG nicht vereinbar, da die Erhebung von personenbezogenen Daten bei einer Auskunftei nur erfolgen darf, wenn die Kenntnis der Daten im Einzelfall für die Beurteilung der Kreditwürdigkeit der Betroffenen unmittelbar relevant ist. Dies war jedoch nicht der Fall, da konkrete Kreditentscheidungen hinsichtlich der Rechtsanwaltskanzleien, über die das Kreditinstitut Bonitätsauskünfte eingeholte hatte, nicht zu treffen waren. Die Maßnahme diente lediglich internen Zwecken des Kreditinstituts. Das Kreditinstitut hat damit die Möglichkeit, Einzelabfragen bei der Auskunftei zu tätigen, zu anderen als den von § 29 BDSG gebilligten Zwecken genutzt. Bei Beachtung der notwendigen Sorgfalt und einer datenschutzgerechteren Gestaltung der innerbetrieblichen Organisation hätte sie dies erkennen und eine andere Maßnahme zur Qualitätssicherung treffen können.

6.3 Auswertung von Girokontodaten

Eine Auswertung der Umsätze von Girokontodaten durch Kreditinstitute mit dem Ziel, den Kunden Angebote zu Vermögensanlagen oder Versicherungen zu unterbreiten, ist nach § 28 Abs. 1 BDSG unzulässig.

Im Berichtszeitraum erhielten wir zwei Bürgerbeschwerden, die die Ausforschung der Umsätze auf dem Girokonto durch ein Hamburger Kreditinstitut betrafen. In einem Fall hatten sich zwei Mitarbeiter der Sparkasse vor einer Vermögensberatung die Kontobewegungen auf dem Girokonto des Kunden ohne dessen vorherige Einwilligung angesehen und im Gespräch gezielt nach Art der Versicherungen und

Versicherungsgesellschaften gefragt, deren Namen aus den Kontodaten ersichtlich waren. Ziel war es, dem Kunden nahezulegen, Versicherungen bei anderen mit dem Kreditinstitut kooperierenden Gesellschaften anzubieten. Auf Nachfrage des Kunden gaben die Bankmitarbeiter an, bei allen Kundenberatungen so vorzugehen. Der Kunde fühlte sich durch das Einsehen in seine Girokontobewegungen erheblich in seiner Privatsphäre verletzt und wird das Girokonto kündigen.

Im zweiten Fall beschwerte sich ein Ehepaar, das Festgeldanlagen wegen der besseren Konditionen bei einem anderen Kreditinstitut unterhielt, darüber, dass ihr Kundenbetreuer gezielt ihr Girokonto auswertete und immer dann Kontakt zu ihnen aufnahm, wenn Umsätze zwischen ihrem Girokonto und dem Kreditinstitut mit den Festgeldanlagen erfolgten. Der Kundenbetreuer rief sie an und bot an, die Gelder bei dem Kreditinstitut selbst anzulegen. Das Ehepaar fühlte sich durch diese Vorgehensweise belästigt.

Die Auswertung von Girokontobewegungen durch ein Kreditinstitut zu Werbe- und Akquisitionszwecken stellt eine unzulässige Nutzung von personenbezogenen Daten dar (vgl. bereits 18. TB Ziffer 24.3) Für die Durchführung des Girokontovertrags ist diese Auswertung nicht erforderlich und daher nicht nach § 28 Abs. 1 Nr. 1 BDSG zulässig. Wegen der entgegenstehenden Interessen der Kunden ist die Auswertung auch nicht nach § 28 Abs. 1 Nr. 2 BDSG zulässig. Der Auswertung von Girokontobewegungen ohne eine entsprechende Einwilligung des Kunden stehen regelmäßig dessen schutzwürdige Interessen entgegen. Der Kunde vertraut darauf, dass das Kreditinstitut die teilweise sehr sensiblen Daten, die eine Kenntnis der Lebensumstände des Kunden ermöglichen, nur im Zusammenhang mit der Durchführung von Transaktionen zur Kenntnis nimmt. Ohne das Wissen und den eindeutigen Willen des Kunden, der eine Beratung wünscht, darf eine Auswertung der Girokontobewegungen nicht erfolgen. Eine darüber hinausgehende Auswertung der Daten verletzt die Privatsphäre der Kunden und erschüttert ihr Vertrauen in einen sorgsamen Umgang mit ihren Daten.

Wir haben das Kreditinstitut auf die datenschutzrechtliche Unzulässigkeit des Verfahrens hingewiesen. Das Kreditinstitut teilte mit, dass dort bekannt sei, dass eine Auswertung der Umsatzdaten eines Girokontos ohne eine entsprechende Einwilligung des Kontoinhabers nicht zulässig sei und verwies beim ersten Fall darauf, dass es sich um einen bedauerlichen Einzelfall gehandelt habe. Man würde diesen Vorfall zum Anlass nehmen, die Kundenberater erneut auf die datenschutzrechtlichen Anforderungen hinzuweisen. Dies scheint jedoch nicht in ausreichender Form erfolgt zu sein, denn der zweite Fall zeigte, dass weiterhin durch Mitarbeiter des Kreditinstituts Girokontobewegungen ausgeforscht worden sind.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit wendet sich entschieden gegen eine Auswertung der Kontodaten durch das Kreditinstitut. Leider ist es nach den Bußgeldvorschriften des Bundesdatenschutzgesetzes nicht möglich, wegen der unzulässigen Nutzung von personenbezogenen Daten ein Bußgeld gegen das Kreditinstitut zu verhängen. Der Gesetzgeber hat die Forderung des Bundesrates, auch die unzulässige Nutzung mit einem Bußgeld zu ahnden, leider bei der letzten Novellierung nicht aufgegriffen. Sollte es erneut zu derartigen Beschwerden gegen das Kreditinstitut kommen, werden wir die Bürger daher darüber unterrichten, dass der Datenschutz durch das Kreditinstitut nicht gewährleistet ist.

7. Handel

7.1 Kundenkarten für Kinder und Jugendliche

Durch Kundenkarten für Kinder und Jugendliche erhält der Einzelhandel detaillierte Informationen über deren Kaufverhalten.

Besorgte Eltern wiesen darauf hin, dass ein großer Hamburger Drogeriemarkt eine Kundenkarte für Kinder und Jugendliche ab 12 Jahren anbot und in den Kartenanträgen eine Vielzahl von Daten verlangte, die das Freizeitverhalten und das Familienumfeld betrafen. Mit der Karte wird über ein Bonuspunktesystem den Karteninhabern beim Einkauf ein Rabatt gewährt, der nach Erreichen einer bestimmten Punktzahl eingelöst werden kann.

Die Unterschrift der Erziehungsberechtigten wurde nicht zwingend verlangt. Auf seiner Internetseite wies das Unternehmen darauf hin, dass der Antrag ohne Unterschrift eines Erziehungsberechtigten ausgefüllt werden dürfe.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit steht Kundenbindungsprogrammen für Minderjährige, die diese bereits daran gewöhnen, private Daten an Unternehmen gegen finanzielle Anreize weiterzugeben, sehr kritisch gegenüber. Während sich viele Erwachsene bewusst gegen Kundenkarten entscheiden, um ihr Kaufverhalten nicht transparent zu machen (gläserner Konsument), ist Jugendlichen die Möglichkeit, dass mithilfe ihrer Daten Profile über ihr Kaufverhalten angefertigt werden können, meist nicht bewusst. Nicht alle Jugendlichen, für die das Angebot gilt, sind aufgrund ihres Reifegrades und ihrer Einsichtsfähigkeit in der Lage, darüber zu entscheiden, ob sie lieber anonym einkaufen oder ihr Kaufverhalten transparent machen wollen und werden durch die Ausgabe der Kundenkarten durch finanzielle Anreize dazu verleitet, ihre Daten weiterzugeben. Ab welchem Alter Kinder und Jugendliche selbst in der Lage sind, Ihre Datenschutzrechte auszuüben und datenschutzrechtlich relevante Sachverhalte zu überblicken, ist bisher nicht geregelt. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ist der Auffassung, dass zumindest Kinder, die noch nicht 14 Jahre alt sind, die notwendige Einsichtsfähigkeit in dieser Hinsicht grundsätzlich nicht haben. Nach den Teilnahmebedingungen bei anderen Bonuskarten müssen die Karteninhaber in der Regel mindestens 16 Jahre alt sein bzw. darf die Karte bei Minderjährigen nur mit Zustimmung der Erziehungsberechtigten ausgegeben werden.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hält eine Verarbeitung der Daten von Jugendlichen ab 12 Jahren im Rahmen der zivilrechtlichen Gestaltung der Karten des Hamburger Unternehmens für zulässig, wenn nur die Daten erhoben, verarbeitet und genutzt werden, die für die Vertragsdurchführung unbedingt erforderlich sind. Bei der Bewertung wurde der so genannte Taschengeldparagraph § 110 BGB berücksichtigt. Danach dürfen Minderjährige, die das 7. Lebensjahr vollendet haben, ohne Zustimmung ihrer gesetzlichen Vertreter vertragsgemäße Leistungen mit Mitteln bewirken, die ihnen zu diesem Zweck oder zu freier Verfügung überlassen worden sind. Auch wenn es bei der Ausübung der Datenschutzrechte um Willenserklärungen geht, die auf tatsächliche Handlungen und nicht auf Rechtsgeschäfte gerichtet sind, wird die im engen Zusammenhang mit derartigen Käufen stehende Datenverarbeitung zum Sammeln von Geldgutscheinen nach § 28 Abs. 1 Nr. 1 BDSG bei Kindern und Jugendlichen ab 12 Jahren als zulässig erachtet, soweit sie sich auf den Namen, die Anschrift und das Ge-

burtsdatum und eine für evtl. Rückfragen erforderliche Telefonnummer oder Email-Adresse beschränkt.

Demgegenüber ist eine Erhebung von Daten mit Angaben zu Hobbies, Freizeitverhalten, Freunden und Familie, die zur Durchführung des Vertrags nicht erforderlich sind, nur mit zusätzlicher Einwilligung der Jugendlichen zulässig. Dies setzt voraus, dass das Unternehmen sie klar und verständlich darüber unterrichtet, dass diese Angaben freiwillig sind und zu welchen Zwecken diese Angaben genutzt werden sollen. Die Jugendlichen müssen darüber hinaus die Einsichts- und Urteilsfähigkeit haben, um den Umfang dieser Datenerhebung und Verarbeitung, die den Werbezwecken des Unternehmens dient, zu überblicken. Diese Einsichtsfähigkeit liegt nach Auffassung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zumindest bei Kindern unter 14 Jahren nicht vor. Konkrete Angaben über Freunde und Familie dürfen jedoch in keinem Fall erhoben werden. Nach § 4 Abs. 2 BDSG sind Daten bei den Betroffenen selbst zu erheben.

Das Unternehmen hat große Bereitschaft gezeigt, in datenschutzrechtlich zulässiger Weise zu agieren, und hat unsere datenschutzrechtlichen Forderungen umgesetzt. Die Unterlagen für die Kundenkarte für Kinder und Jugendliche wurden umgestaltet und so mehr Transparenz für die Nutzergruppe geschaffen. Es ist nun generell für die Beantragung der Karte und die damit verbundene Weitergabe von personenbezogenen Daten eine Einverständniserklärung der Erziehungsberechtigten bei Antragstellern unter 12 Jahren vorgesehen. Darüber hinaus müssen Eltern bei Antragstellern unter 14 Jahren eine weitere schriftliche Einwilligung erteilen, wenn die Kinder freiwillige Angaben für die Durchführung von Werbeaktionen machen.

7.2 Weitergabe von Kundendaten bei Geschäftsaufgabe

Eine Weitergabe von Kundendaten bei Geschäftsaufgabe an ein Unternehmen, das künftig die Belieferung des Kunden vornehmen soll, ist nur dann zulässig, wenn die Kunden vorab über die Weitergabe unterrichtet werden und ihnen zumindest ein Widerspruchsrecht eingeräumt wird.

Durch Beschwerden wurden wir darauf aufmerksam, dass ein Energielieferant in Hamburg wegen Geschäftsaufgabe seinen gesamten Kundenstamm einschließlich der Konto- und Verbrauchsdaten an ein anderes Hamburger Energieversorgungsunternehmen weitergegeben hatte. Die Kunden wurden durch das Unternehmen darüber informiert, dass es die Tätigkeit als Stromlieferant einstelle und den Kundenstamm an das andere Unternehmen übertragen werde. Wenige Tage später erhielten die Kunden von dem neuen Energielieferanten ein Begrüßungsschreiben. Eine Möglichkeit, der Weitergabe ihrer Kundendaten zu widersprechen, gab es nicht mehr, da die Weitergabe der Daten bereits erfolgt war. Betroffen waren die Daten von mehr als 3500 Kunden. Mehr als 500 dieser Kunden haben sich gegen eine Belieferung durch das neue Energieversorgungsunternehmen entschlossen und von diesem die Löschung ihrer Daten verlangt, was unverzüglich erfolgte.

Der Energieversorger war nach den Vorschriften des BDSG nicht berechtigt, wegen Geschäftsaufgabe die Kundendaten einschließlich der Kontodaten an einen anderen Energieversorger weiterzugeben. Eine Rechtsgrundlage für die Weitergabe der Kundendaten lag nicht vor. Das Unternehmen hatte sich zur Rechtfertigung der Datenweitergabe auf eine Ziffer in seinen AGB berufen. Danach war es berechtigt, Rechte und Pflichten aus dem Vertrag an einen Dritten abzutreten oder Dritte mit der Erbringung von Leistungen oder einem Teil von Leistungen zu beauftragen.

Nach unserer Auffassung stellte diese AGB jedoch keine Rechtsgrundlage für die Weitergabe der Kundendaten dar, da sie nur Beauftragungen Dritter im Rahmen der Vertragsdurchführung betraf. Die Veräußerung und Weitergabe der Kundendaten infolge der Geschäftsaufgaben an ein anderes Untenehmen war davon nicht erfasst. Das neue Unternehmen erbrachte keine Rechte und Pflichten aus dem ursprünglichen Vertrag, sondern es erbrachte im eigenen Namen und für eigene Rechnung Leistungen an die Kunden. Daher war die Datenweitergabe nicht nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG berechtigt.

Die Datenweitergabe war auch nicht nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig, da die schutzwürdigen Interessen der Kunden gegen eine Weitergabe ihrer Daten höher zu bewerten waren als die Interessen der beteiligten Stromversorgungsunternehmen. Die Kunden wurden vor vollendete Tatsachen gestellt. Ihnen wurde keine Widerspruchsmöglichkeit gegen die Weitergabe ihrer Daten eingeräumt, obwohl dies ohne Weiteres möglich gewesen wäre.

Wegen der besonderen Umstände, insbesondere dem auf die AGB zurückzuführenden Irrtum des Unternehmens und seinen Bemühungen mit dem neuen Stromlieferanten, die über 500 nachträglichen Widersprüche unverzüglich zu berücksichtigen, haben wir in diesem Einzelfall von der Verhängung eines Bußgeldes gegen die beteiligten Unternehmen abgesehen.

7.3 Veröffentlichung von Kundendaten im Internet durch Internetbuchhändler

Datenpannen im zertifizierten Online-Shop zeigen, dass der Kunde trotz Gütesiegel nicht immer beruhigt einkaufen kann. Der Gesetzgeber ist gefordert.

Durch eine Beschwerde wurden wir darauf aufmerksam, dass beim Internet-Buchgroßhändler Libri über mehrere Monate Rechnungsdaten von mehreren hunderttausend Kunden ungesichert im Internet standen. Da die Kunden-URL sich nur durch einen fortlaufend gebildeten numerischen Parameter unterschieden, konnte sich ein Nutzer mit wenig Aufwand nach Auswahl der Rechnungsanzeigefunktion auf der Webseite des Händlers eine andere Rechnung durch Ändern der Nummer am Ende der URL anzeigen lassen. Die Rechnungen enthielten die Rechnungsadresse, Lieferadresse, Bestelldaten wie Titel der Bücher, Name der Partnerbuchhandlung und die Bezahlart, jedoch keine Bank- und Kreditkartendaten. Unmittelbar nach Kenntnisnahme der Datenlücke reagierte das Unternehmen und beseitigte den Mangel durch Deaktivierung und anschließende Umprogrammierung der Funktionalität. Nach Mitteilung des Unternehmens war die Funktionalität zur Anzeige von Rechnungen von einem Dienstleister entgegen den Vorgaben falsch implementiert worden.

Die Webseite www.libri.de enthielt ein am 7. Mai 2009 vom TÜV Süd ausgestelltes „s@fer-shopping" Zertifikat. Darin wurde auf die Sicherheit von personenbezogenen Daten der Online-Kunden und die Durchführung eines „Datenschutz-Kurzchecks" hingewiesen. Das Gütesiegel wird vom TÜV Süd an Online-Shops vergeben. Auf seiner Webseite weist der TÜV Süd darauf hin, dass der Kunde, der das Prüfzeichen sieht, beruhigt im Online-Shop einkaufen könne, da der Händler sorgfältig geprüft worden sei. Dabei seien von Interesse, ob die Bestellabwicklung zuverlässig abgewickelt, Anfragen ernst genommen und die persönlichen Daten geschützt würden sowie ob die Zahlungsabwicklung sicher sei. Neben einer ausführlichen Online-Bewertung schaue sich der TÜV Süd die Stellen auch vor Ort an.

Bei der weiteren Aufklärung der Angelegenheit stellte sich heraus, dass die Prüfung des Libri-Online-Shops durch den TÜV Süd bereits vor dem Einsatz der Software mit der fehlerhaften Rechnungsfunktionalität ab Mitte 2008 erfolgte, so dass der Fehler damals nicht erkannt werden konnte. Libri hatte nach der Hauptprüfung durch den TÜV ein Update durchgeführt, bei dem die notwendige Absicherung in der Rechnungsschnittstelle vergessen wurde. Die Nachprüfungen des TÜV bis zur Erteilung des Siegels im Mai 2009 betrafen jedoch nur die Behebung der Mängel, die bei der Hauptprüfung festgestellt worden waren und nicht danach installierte Softwareversionen.

Dieser Vorfall lässt viele Fragen offen. Insbesondere bleibt zu klären, ob der Einsatz einer neuen Software nicht hätte erneut überprüft werden müssen. Der TÜV Süd hat dazu erklärt, dass der Kunde nach dem Verfahren zu eigenständigen Qualitätskontrollen verpflichtet sei. Nach Bekanntwerden der Sicherheitslücke bei Libri habe man alle Kunden, die derzeit nach s@fer-shopping zertifiziert seien, überprüft und dabei ähnliche Probleme in Folge von Updates festgestellt und diese umgehend beseitigt. Die TÜV Süd AG habe daher beschlossen, verstärkt außerplanmäßige Sicherheitsprüfungen bei zertifizierten Unternehmen durchzuführen. Außerdem würde derzeit die Umsetzung einer Meldepflicht für Updates geprüft.

Kurz nach Bekanntwerden der Datenlücke, die die direkten Libri-Kunden betraf, erhielten wir den Hinweis, dass auch Konten von Buchhändlern, denen Libri auf seiner Webseite eigene Onlineshops zur Verfügung stellt, nicht hinreichend gesichert waren. Die Stores enthalten Angaben über ca. 1000 Buchhändler und deren Buchbestellungen bei Libri. Aufgeführt sind hier auch die Kundenlisten von Buchhändlern mit Namen, Postanschrift und E-Mailadressen. Neben dem Umsatz der einzelnen Kunden sind das Datum der Bestellung sowie die Buchtitel vermerkt, die die Kunden über die Buchhändler bestellt haben.

Im Rahmen der jeweiligen Einrichtung eines Shops für die Buchhändler vergibt Libri dem Buchhändler individuelle initiale Zugangsdaten mit der Aufforderung, das Passwort unverzüglich zu ändern. Zu der Zugriffsmöglichkeit durch Dritte kam es, weil die von Libri verteilten Initialpasswörter laufende Nummerierungen enthielten. Anhand der Daten eines Shops ließen sich leicht die Passwörter anderer Shops, die keine Änderungen der Initialpasswörter vorgenommen hatten, erraten. Von dieser Zugriffsmöglichkeit waren Kunden von lokalen Buchhändlern betroffen, die entgegen der Aufforderung durch Libri ihr Passwort nicht geändert hatten. Auch in diesem Fall fand eine Zertifizierung durch den TÜV Süd statt, die sich jedoch nicht auf die explizite Überprüfung der Buchhändlerpassworte bezog.

Libri sperrte umgehend nach Bekanntwerden der Datenlücke den Zugang über das Internet zu dem betroffenen System. Die Passwörter aller das System nutzenden Buchhändler wurden geändert. Künftig ist systemseitig vorgegeben, dass jeder Benutzer nach dem ersten Login das von Libri vergebene Passwort sofort ändern muss.

Es ist positiv zu erwähnen, dass Libri auf die Pannen schnell reagierte und im Rahmen des Krisenmanagements die Datenlecks umgehend geschlossen hat. Dennoch dokumentieren die Erkenntnisse in dieser Angelegenheit ein erhebliches Ausmaß an Unkenntnis und Nachlässigkeit im Umgang mit personenbezogenen Daten und der Datensicherheit. Es waren nicht die technischen Maßnahmen getroffenen worden, die nach §9 BDSG zur Sicherstellung der Anforderungen des Datenschutzes erforderlich gewesen wären. Dies gilt sowohl für die nicht ausreichende technische Absicherung der Rechnungsschnittstelle im Libri-Online-Shop als auch

für die Vergabe von Initialpasswörtern für die Buchhändler durch Libri. Deren simple numerischen Parameter hätten die Store-Betreiber geradezu einladen können zu testen, ob es möglich sei, der Konkurrenz in die Karten zu schauen. Das gilt aber auch für die Storebetreiber selbst, die ihre geschäftlichen Daten offenbar für so wenig schützenswert erachtet haben, dass sie auf eine Änderung des von Libri erteilten Zugangspassworts für ihren Store verzichteten. Dass sie dadurch auch die persönlichen Daten ihrer Kunden gefährdet haben, ist nicht hinnehmbar.

Beide Fälle offenbaren eine Kette von erheblichen Pannen mit unterschiedlichen Beteiligten. Am Ende der Kette stand letztlich der Kunde, um dessen Datensicherheit sich nicht gekümmert wurde.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ist der Auffassung, dass künftig eine aktuelle datenschutzkonforme Zertifizierung stattfinden muss, um dem Vertrauen der Bürger in derartige Zertifikate Rechnung zu tragen. Dabei müssen auch Updates zwingend berücksichtigt werden. Außerdem zeigen auch diese Vorfälle, dass der Gesetzgeber aufgefordert ist, für die Durchführung von Datenschutzaudits klare und einheitliche Maßstäbe zu schaffen. Gleiches gilt für einen bereits seit langem geforderten Bußgeldtatbestand bei Vorliegen von technischen und organisatorischen Mängeln im Bereich der Datensicherheit. Beide Forderungen werden seit langem von den Datenschutzbeauftragten erhoben.

8. Werbung

8.1 Werbung

Grundsatz der Einwilligung statt Listenprivileg – zum Vorteil der Betroffenen?

Personenbezogene Daten sind längst zu einer Handelsware geworden. In diesem Kampf um Marktanteile zählt der Schutz der informationellen Selbstbestimmung immer weniger. Umso wichtiger ist es für jeden Einzelnen, seine Rechte zu kennen und wahrzunehmen. Bislang durften Unternehmen eine begrenzte Zahl von Daten – so genannte Listdaten -, darunter Name, Anschrift, Geburtsjahr, Beruf sowie akademische Grade und Titel nutzen, wenn der Betroffene dieser Verwendung nicht ausdrücklich widersprochen hat. Die Datenschutzbeauftragten des Bundes und der Länder hatten immer gefordert, dieses Prinzip umzudrehen:

Der Handel mit persönlichen Daten sollte generell nur noch dann erlaubt sein, wenn die Betroffenen ausdrücklich zugestimmt haben. Der Handel mit personenbezogenen Daten ohne eine solche Zustimmung sollte verboten sein.

Unter dem Eindruck der Skandale der vergangenen Monate um den groß angelegten Missbrauch personenbezogener Daten hat nun auch der Gesetzgeber reagiert. Die Änderungen traten zum 1. September 2009 in Kraft.

Was ist ab dem 1. September 2009 erlaubt?

Grundsätzlich dürfen personenbezogene Daten nur mit Einwilligung des Betroffenen zu Zwecken der Werbung und des Adresshandels verarbeitet oder genutzt werden. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, muss sie jetzt in drucktechnisch deutlicher Gestaltung besonders hervorgehoben werden.

Wird von dem Schriftformerfordernis nach § 4a BDSG abgewichen, hat die verantwortliche Stelle den Inhalt der Einwilligung dem Betroffenen schriftlich zu bestätigen, es sei denn, dass sie elektronisch erklärt wird (§ 28 Abs. 3a BDSG).

Von dem Erfordernis der Einwilligung hat der Gesetzgeber viele Ausnahmen vorgesehen. Ohne Einwilligung kann Werbung insbesondere dann versandt werden, wenn der Betroffene anhand der Werbung erkennen kann, welches Unternehmen seine Adressdaten hierfür weiterverkauft hat. Dazu müssen Herkunft und Weitergabe der Adressdaten dokumentiert werden. Bereits aus der Werbung selbst muss für den Betroffenen erkennbar sein, wer seine Daten erstmalig weitergegeben hat. Diese Stelle muss dem Betroffenen dann auf Nachfrage mitteilen können, an wen sie seine Daten zu Werbezwecken in den letzten zwei Jahren weitergegeben hat. Hierfür gewährt der Gesetzgeber eine Übergangsfrist. Erst ab dem 1. April 2010 ist diese Pflicht verbindlich.

- Ohne Einwilligung dürfen Unternehmen auch ihre bisherigen Kunden bewerben, sofern sie ausschließlich die Listdaten nutzen. Eine Zuspeicherung von Daten ist jedoch erlaubt.
- Ohne Einwilligung dürfen Angaben aus allgemein zugänglichen Adress-, Rufnummern- oder Branchenverzeichnissen genutzt werden.
- Berufsbezogene Werbung an die berufliche Anschrift bedarf keiner Einwilligung.
- Auch Spendenwerbung gemeinnütziger Organisationen bedarf keiner Einwilligung, wenn lediglich Listdaten genutzt werden.

Das Gesetz sieht für die von den Änderungen betroffenen Unternehmen eine Übergangsfrist von drei Jahren vor. Für Daten, die vor dem 1. September 2009 erhoben wurden, gilt daher die alte Rechtslage zunächst fort, d. h.:

- Daten, insbesondere Name, Anschrift, Geburtsjahr, Beruf sowie akademische Grade und Titel können ohne Einwilligung des Betroffenen weiter wie bisher genutzt werden, und zwar
- für Zwecke der Markt- oder Meinungsforschung bis zum 31. August 2010 und
- für Zwecke der Werbung bis zum 31. August 2012.

8.2 Telefonwerbung

Die neuen Möglichkeiten der Bundesnetzagentur – hat die unerwünschte Telefonwerbung bald ein Ende?

Seit Jahren ist die Telefonwerbung – erst durch ständige Rechtsprechung des Bundesgerichtshofes, dann im Jahr 2004 im Gesetz gegen den unlauteren Wettbewerb (UWG) geregelt – ohne Einwilligung des Betroffenen unzulässig. Das hat viele Unternehmen jedoch nicht davon abgehalten, Verbraucher mit so genannten „Cold Calls" in teilweise sehr aggressiver Form zu „überfallen". Die seit August 2009 geltenden neuen Regelungen sollen helfen, den Verbraucher vor unerbetenen Anrufen besser zu schützen:

- Verstöße gegen das bestehende Verbot der unerlaubten Telefonwerbung gegenüber Verbraucherinnen und Verbrauchern können mit einer Geldbuße bis zu 50.000 Euro geahndet werden.

- Anrufer bei Werbeanrufen dürfen ihre Rufnummer nicht mehr unterdrücken, um ihre Identität zu verschleiern. Bei Verstößen gegen das Verbot droht eine Geldbuße von bis zu 10.000 Euro.

Die genannten Ordnungswidrigkeiten können von der Bundesnetzagentur geahndet werden:

Bundesnetzagentur, Tulpenfeld 4, 53113 Bonn, www.bundesnetzagentur.de.

Die Bundesnetzagentur hält ein Formular bereit, mit dem Verbraucher Anzeige erstatten können, wenn sie unerlaubte Telefonwerbung erhalten. Aus diesem Formular geht hervor, welche Angaben die Bundesnetzagentur benötigt, damit sie das Bußgeldverfahren durchführen kann.

Während das Wettbewerbsrecht nun ein ausdrückliches Einverständnis, aber ohne Schriftformerfordernis vorsieht, ist aus datenschutzrechtlicher Sicht die Nutzung oder Übermittlung der Telefonnummer grundsätzlich nur mit einer schriftlichen Einwilligung erlaubt (s. Kap. IV 8.1).

9. Arbeitnehmerdatenschutz

9.1 Abgleich von Kontodaten von Mitarbeitern und Lieferanten

Bei der Verarbeitung und Nutzung von Mitarbeiterdaten für interne Finanzkontrollmaßnahmen zur Korruptionsbekämpfung müssen die Vorschriften des BDSG beachtet werden.

Im April 2009 wurde in der Öffentlichkeit bekannt, dass durch die in Hamburg ansässige Airbus Deutschland GmbH die Kontodaten von mehr als 20.000 Airbus-Mitarbeitern mit den Kontodaten von Lieferanten zur Korruptionsbekämpfung im Zeitraum zwischen 2005 und Juli 2007 mehrmals abgeglichen wurden. Dabei wurden Datensätze der Mitarbeiter, die die jeweilige Personalnummer, die Kontonummer und die Bankleitzahl enthielten, mit Datensätzen der Lieferanten bestehend aus Name, Kontonummer und Bankleitzahl abgeglichen. Nach Angaben des Unternehmens diente der Abgleich der Überprüfung, ob Mitarbeiter zusätzlich zu ihrer Beschäftigung im Unternehmen in gewerblicher Tätigkeit Waren an Airbus liefern oder Airbus gegenüber Dienstleistungen erbringen. Es sollte festgestellt werden, ob Mitarbeiter sich selbst Aufträge erteilen oder an solchen Aufträgen mitwirken. Darüber hinaus sollte der Kontenabgleich die Feststellung ermöglichen, ob angestellte Mitarbeiter als externe Dienstleister oder Lieferanten Leistungen erbringen, die zu ihren Aufgaben als Mitarbeiter gehören und durch solche Tätigkeiten gegen die vertraglich vereinbarte Genehmigungspflicht für Nebentätigkeiten verstoßen. Im Rahmen des Kontoabgleichs wurde eine geringe Anzahl von individuellen Übereinstimmungen von Gehaltskonten mit Lieferantenkonten festgestellt. In diesen Fällen erfolgte eine Rückführung auf die Mitarbeiternamen. Die Fälle wurden zunächst von den zuständigen Personalmitarbeitern und soweit erforderlich unter Einbeziehung der Leiter der Einkaufsabteilung und der Abteilung Geschäftsbuchhaltung geklärt. Ein Fehlverhalten von Mitarbeitern wurde in keinem der Fälle festgestellt. Alle Einzelfälle der Doppelerfassung konnten durch plausible Gründe belegt werden. Das Verfahren wurde im Juli 2007 letztmalig angewandt und danach eingestellt.

Die aufsichtsbehördliche Prüfung ergab, dass die Kontenabgleiche ohne ausreichende Beteiligung des Betriebsrats erfolgt waren. Die datenschutzrechtlich relevanten Regelungen einer Konzernbetriebsvereinbarung vom Januar 2006 zur Ein-

führung eines alljährlich stattfindenden Financial Control Health Check Audits waren weder mit Blick auf den Inhalt, worauf sich die Prüfung bezieht, noch auf den zeitlichen Umfang aussagekräftig und konnten nicht als Rechtsgrundlage für die Nutzung der Arbeitnehmerdaten herangezogen werden. Die Kontenabgleiche erfolgten auch ohne Einbeziehung des betrieblichen Datenschutzbeauftragten. Sie hatten weder einen konkreten Anlass, noch wurden sie in korruptionsanfälligen Bereichen durchgeführt und betrafen eine Vielzahl von Mitarbeitern ohne deren Wissen. In keinem der wenigen Fälle, in denen eine Übereinstimmung der Kontodaten vorlag, konnte ein individuelles Fehlverhalten der Arbeitnehmer festgestellt werden. Die durch das Screening bewirkte nicht unwesentliche Beeinträchtigung des informationellen Selbstbestimmungsrechts der Arbeitnehmer im Rahmen des von Airbus durchgeführten Massenverfahrens lässt sich durch den Zweck der Korruptionsprävention nicht rechtfertigen. In der Gesamtabwägung nach § 28 Abs. 1 BDSG war somit von einer datenschutzwidrigen Praxis durch Airbus auszugehen.

Die Erhebung eines Bußgeldes musste unterbleiben, da für die unzulässige Nutzung von Arbeitnehmerdaten keine gesetzliche Grundlage gegeben ist (siehe dazu auch Ziffer 6.3). Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat das Unternehmen aufgefordert, dafür Sorge zu tragen, bei allen laufenden und künftigen Nutzungen von Mitarbeiterdaten für interne Finanzkontrollmaßnahmen die Vorschriften des BDSG zu beachten.

9.2 Präventionsmaßnahmen nach § 32 BDSG

Maßnahmen durch den Arbeitgeber zur Verhinderung von Regelverstößen und Straftaten sind unter bestimmten Voraussetzungen möglich.

Durch die Neuregelung des § 32 Abs 1 Satz 2 BDSG hat der Gesetzgeber klargestellt, dass Beschäftigtendaten nur dann zur Aufdeckung von Straftaten erhoben, verarbeitet oder genutzt werden dürfen, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht einer Straftat im Beschäftigungsverhältnis begründen. Diskutiert wird darüber, inwieweit der neu geschaffene § 32 BDSG auch auf Präventionsmaßnahmen durch den Arbeitgeber anzuwenden ist. Entsprechend der Gesetzesbegründung zu § 32 Abs. 1 Satz 1 BDSG ist die Zulässigkeit von Maßnahmen, die zur Verhinderung von Straftaten oder sonstigen Rechtsverstößen, die mit dem Beschäftigungsverhältnis im Zusammenhang stehen, nach § 32 Abs. 1 Satz 1 BDSG zu beurteilen.

Eine personenbezogene Datenerhebung, -verarbeitung und -nutzung ist jedoch nur zulässig, wenn sie erforderlich ist. Folgende Prüfschritte sind dabei zugrunde zu legen:

- Welche Beschäftigten sind von einer präventiven Kontrolle betroffen?
- Welche Ziele sollen mit präventiven Kontrollen verfolgt werden?
- Sind diese Ziele auch ohne personenbezogene Datenverarbeitung zu erreichen, entsprechend dem Grundsatz des § 3a BDSG?
- Welche anderen, in geringerem Maße in das Persönlichkeitsrecht des Betroffenen eingreifende Maßnahmen sind zur Erreichung der Zwecke möglich?
- Hat das Unternehmen eine Gefährdungsanalyse erstellt, in welchen Bereichen es zu Pflichtverletzungen und Verstößen kommen kann?

Ein pauschales Screening von Mitarbeiterdaten ohne konkreten Anlass ist daher nach § 32 BDSG nicht zulässig.

Der betriebliche Datenschutzbeauftragte und der Betriebsrat sind vor der Einführung einer präventiven Kontrollmaßnahme zu beteiligen.

Unabhängig davon fehlen angesichts des komplexen Spannungsverhältnisses zwischen betrieblicher Kontrolle zur Korruptionsbekämpfung und Arbeitnehmerdatenschutz jedoch nach wie vor klare Kriterien für das, was erlaubt ist. Die Forderung nach einem Arbeitnehmerdatenschutzgesetz steht daher weiterhin auf der Tagesordnung und wird zukünftig ein zentrales Anliegen des Datenschutzes bleiben.

9.3 Betriebsvereinbarung als vorrangige Rechtsvorschrift

Die Parteien Arbeitgeber und Betriebsrat können die Anforderungen des Bundesdatenschutzgesetzes nicht unterschreiten.

Im Berichtszeitraum wurden wir mehrfach aufgrund von Beschwerden auf Datenverarbeitungen von Beschäftigtendaten aufmerksam, deren Zulässigkeit auf einer Betriebsvereinbarung beruhen sollte. Prüfungen ergaben jedoch, dass der Erlaubnistatbestand Betriebsvereinbarung als vorrangige Rechtsvorschrift im Sinne § 4 Abs. 1 BDSG nicht herangezogen werden konnte. Aus datenschutzrechtlicher Sicht fehlten vielfach grundlegende Regelungen zur personenbezogenen Datenverarbeitung.

Die Vertragsparteien Arbeitgeber und Betriebsrat können Vereinbarungen über arbeitsrechtliche Sachverhalte treffen, wobei eine inhaltliche Prüfung nicht zu den Aufgaben einer Aufsichtsbehörde für Datenschutz gehört. Wenn die geregelten Sachverhalte jedoch zur Folge haben, personenbezogene Daten von Beschäftigten zu verarbeiten oder zu nutzen, dann müssen diese Verfahren näher beschrieben werden. Dazu gehören insbesondere

- Gegenstand der Datenverarbeitung
- Zweckbindung
- Datenvermeidung und Datensparsamkeit
- Art und Umfang der verarbeiteten Daten
- Empfänger der Daten
- Rechte der Betroffenen
- Löschfristen
- Technische und organisatorische Maßnahmen wie beispielsweise das Berechtigungskonzept

10. Bußgeldfälle und Strafanträge

Im Berichtszeitraum wurden erneut Bußgelder festgesetzt und Strafanträge gestellt.

Wegen Nichterteilung einer Auskunft (§ 43 Abs. 1 Nr. 10 BDSG) verhängte die Aufsichtsbehörde in 2 Fällen Bußgelder in Höhe von 750 und 1000 Euro. In beiden Fällen wurden die Bußgelder bezahlt. Wegen der unbefugten Erhebung von personenbezogenen Daten durch ein Kreditinstitut (siehe Ziffer IV 6.2) wurde ein Bußgeld von 7.500 Euro verhängt, das ohne Einlegung eines Rechtsbehelfs durch die verantwortliche Stelle beglichen wurde. Gegen ein nach § 43 Abs. 2 Nr. 1 BDSG wegen unbefugter Übermittlung von nicht allgemein zugänglichen Daten im Internet ver-

hängtes Bußgeld in Höhe von 800 Euro wurde Einspruch eingelegt. Das Verfahren ist noch nicht abgeschlossen.

Die Aufsichtsbehörde stellte im Berichtszeitraum 2 Strafanträge. In einem Fall wurden unbefugt Kundendaten zum Verkauf angeboten. Bedauerlicherweise wurde das Verfahren eingestellt. Auch der andere Fall betraf Kundendaten einschließlich Kontodaten. Es bestand der Verdacht auf Datenhandel durch ein Callcenter. Über den Ausgang dieses Strafverfahrens haben wir noch keine Informationen.

11. Meldepflicht und Prüftätigkeit

11.1 Meldepflicht und Register nach § 4d BDSG

Die Zahl der Meldungen ist erneut leicht gestiegen.

Die Aufsichtsbehörde führt nach § 38 Abs. 2 BDSG ein Register der Stellen, die nach § 4d BDSG der Meldepflicht unterliegen. Bisher haben 47 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, 20. TB 30.1, 21. TB, 30.1). Unterteilt nach der Art der meldepflichtigen Verfahren ergibt sich folgendes Bild:

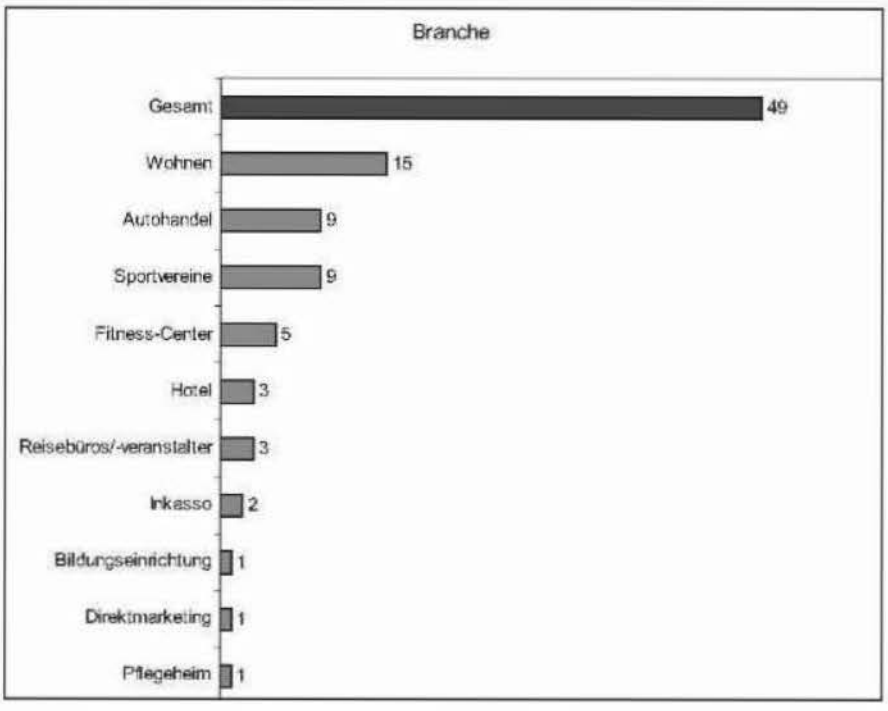
- Speicherung zum Zwecke der Übermittlung
  Auskunfteien/Warndienste 11
  Informationsdienste 4
  Adresshändler 6
- Speicherung zum Zwecke der anonymisierten Übermittlung
  Markt- und Meinungsforschung 26

11.2 Prüfungen

Eine Verbesserung des Datenschutzniveaus konnten wir bei unseren anlassfreien Unternehmensprüfungen gegenüber den Vorjahren leider nicht feststellen.

Im Berichtszeitraum haben wir in insgesamt 49 Unternehmen auf die Einhaltung der datenschutzrechtlichen Bestimmungen überprüft.

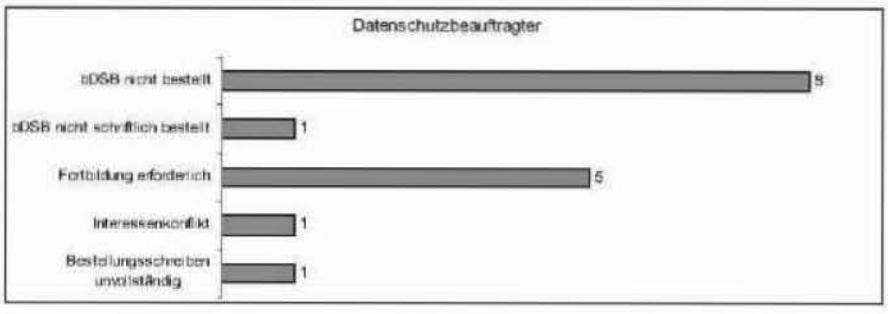
Unsere Kontrollen haben wir in folgenden Bereichen vorgenommen:



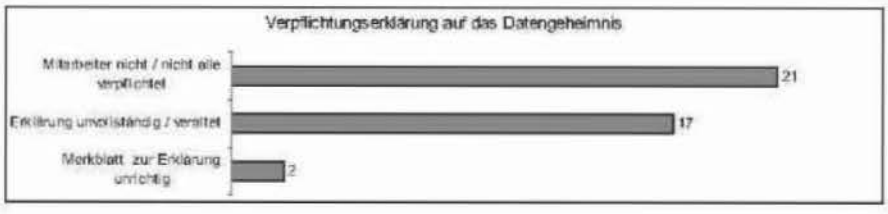
Gegenstand der Prüfungen war vor allem:

- Die Verpflichtung zur Bestellung eines Datenschutzbeauftragten nach § 4f BDSG,
- die Fachkunde des Datenschutzbeauftragten nach § 4g Abs. 1 BDSG,
- das Verfahrensverzeichnis nach § 4g Abs. 2 BDSG,
- die Verpflichtung der Mitarbeiter, die personenbezogene Daten verarbeiten, auf das Datengeheimnis nach § 5 BDSG,
- die erforderlichen technischen und organisatorischen Maßnahmen nach § 9 BDSG,
- die Anforderungen bei einer Auftragsdatenverarbeitung nach § 11 BDSG,
- die Meldepflicht nach § 4d BDSG,
- sowie verstärkt auch die konkreten DV-/Arbeitsprozesse in den geprüften Branchen.

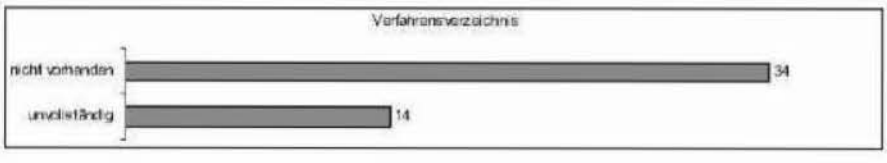
Auch wenn noch nicht alle Prüfungen des Berichtszeitraums 2008/09 abgeschlossen worden sind, muss erneut festgestellt werden, dass keine Prüfung frei von Mängeln war.



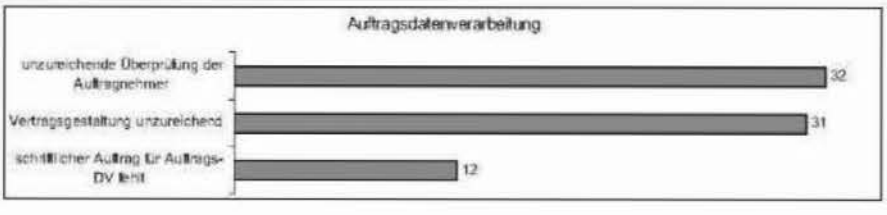
Rund 17 % der geprüften Unternehmen sind ihrer Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten nicht nachgekommen.



Die Verpflichtung auf das Datengeheimnis der beschäftigten Personen, die personenbezogene Daten verarbeiten, fehlte bei ca. 43 % der geprüften Unternehmen.



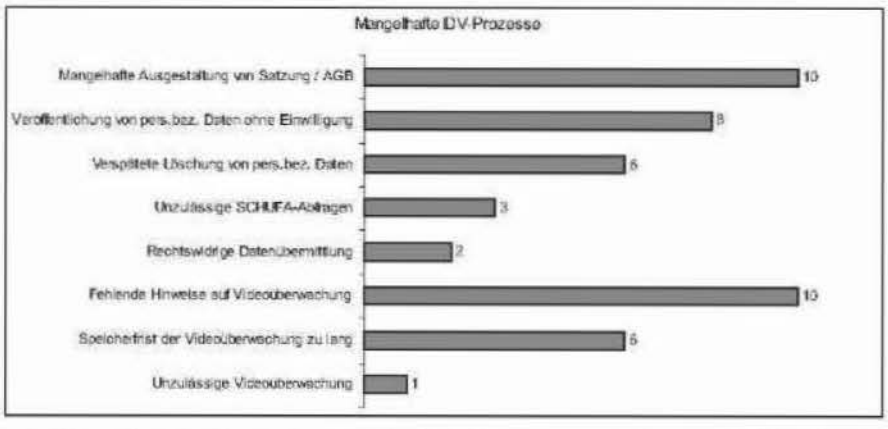
Noch gravierender stellt sich das Bild beim Verfahrensverzeichnis dar. Dieses Verzeichnis soll die Transparenz der Datenverarbeitungsprozesse in einem Unternehmen erhöhen. Es ist von jedem Unternehmen zu führen, sofern personenbezogene Daten verarbeitet werden. Jeder Dritte (nicht nur Kunden, Mitarbeiter, etc.) hat das Recht, diese Informationen einzusehen. Leider mussten wir erneut feststellen, dass die überwiegende Zahl von Firmen (70 %) ihrer gesetzlichen Verpflichtung nicht nachgekommen sind.



Ein ähnlich schlechtes Bild wie beim Verfahrensverzeichnis ergibt sich bei der Ausgestaltung der Auftragsdatenverarbeitung nach § 11 BDSG. Zum 1. September 2009 hat der Gesetzgeber konkretere Forderungen an die Vertragsgestaltung und die Kontrolle der Auftragnehmer verabschiedet. Im Rahmen unserer Prüfungen haben wir die geprüften Unternehmen und Vereine frühzeitig auf die gesetzlichen Änderungen im BDSG hingewiesen. In der Regel waren die Verträge noch nicht angepasst worden.

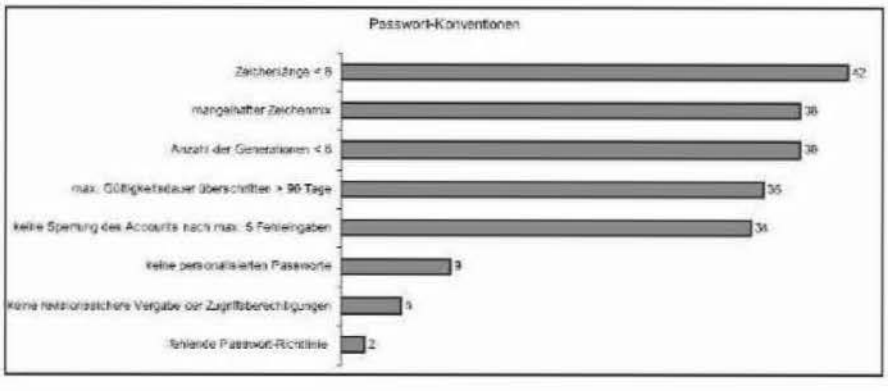
Einer ordnungsgemäßen Vertragsgestaltung und Kontrolle der Auftragnehmer kommt insofern eine besondere Bedeutung zu, da Verstöße nunmehr mit Bußgeldern bis zu 30.000,- Euro durch die Aufsichtsbehörde geahndet werden können.

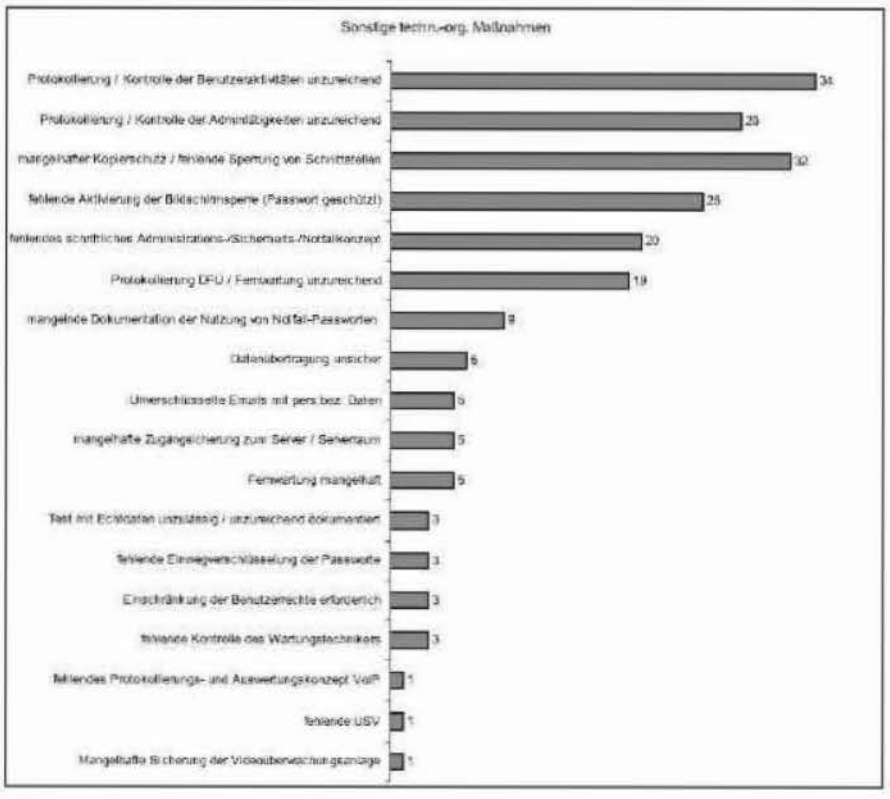
Wir gehen davon aus, dass die Hamburger Unternehmen ihre Verträge zur Auftragsdatenverarbeitung bis zum Ende des 1. Quartals 2010 vollständig überarbeitet und entsprechende Kontroll-Prozesse etabliert haben.



Die Mängelliste bei den konkreten DV-/Arbeitsprozessen ist bunt und vielschichtig. Verallgemeinert dargestellt fehlt es auch hier an einer ausreichenden Transparenz und Information über die konkreten Verarbeitungsprozesse und deren Notwendigkeit.

Auch im Bereich der IT-Sicherheit stellten wir erneut zahlreiche Mängel fest:





Den Empfehlungen zum IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik – BSI – wird offensichtlich von den Unternehmen zu wenig Aufmerksamkeit geschenkt. Auch wenn bei diesen Diagrammen zu berücksichtigen ist, dass eine Vielzahl von einzelnen IT-Verfahren geprüft worden ist, sind die Mängel im Bereich der IT-Sicherheit offenkundig. Wie bereits in der Einleitung zu diesem 22. Tätigkeitsbericht ausgeführt, werden wir unser Prüfkonzept für das Jahr 2010 ändern. Ziel ist es, neben nur noch vereinzelten anlassfreien Prüfungen im bisherigen Stil, die Datenschutzbeauftragten in den Hamburger Unternehmen gezielt durch unsere Ansprache zu stärken, aber auch, deren Unterstützung im Hinblick auf eine Verbesserung des Datenschutzniveaus in der Hamburger Wirtschaft einzufordern. Durch die Unternehmensprüfungen der vergangenen Jahre liegen uns umfangreiche Ergebnisse im Hinblick auf die bedeutendsten Datenschutzmängel vor. Gemeinsam mit den betrieblichen Datenschutzbeauftragten wollen wir versuchen, diese Mängel zu beseitigen.

12. Eingaben

So viele Eingaben wie in diesem Berichtszeitraum hat es bisher noch nicht gegeben.

Von Januar 2008 bis Dezember 2009 gingen 1.982 schriftliche Eingaben ein, eine Steigerung im Vergleich zum Zeitraum Januar 2006 bis Dezember 2007 mit 1.333 um **49 %**. Sie betrafen – getrennt für die Jahre 2008 und 2009 – folgende Datenschutzbereiche:

	2008	2009
Versicherungswirtschaft	29	27
Kreditwirtschaft	31	38
Priv. Wohnungswirtschaft	16	22
Versandhandel	22	18
sonst. Handel	46	58
Werbung, Direktmarketing	159	163
Schufa, Auskunfteien	50	45
Markt- und Meinungsforschung	7	13
Vereine, Parteien	12	20
Freie Berufe	33	54
Soziales u. Gesundheitsw., nicht-öff.	20	21
PersonalDS, nicht-öff.	24	31
Verkehrswesen, nicht-öff.	9	11
Sonstiges, nicht-öff.	49	50
Justiz	10	10
Strafvollzug	14	8
Sicherheitsüberprüfung	-	1
Verfassungsschutz	3	4
Polizei	19	29
Staatsanwaltschaft	5	7
Meldewesen	13	14
Wahlen	3	1
MDK, Kranken- und Pflegedienste	9	7
ALG II	47	38
andere Sozialbereiche	45	19
Gesundheitswesen, öff.	12	16
PersonalDS, öff.	24	26
Sicherheitsbereich	-	0
Verkehrswesen, öff.	3	7
Ausländerwesen	5	0
Finanz- und Steuerwesen	7	8
Bildungswesen	12	20
Wirtschaftsverwaltung	5	3
Telekommunikation	10	32
Tele- und Mediendienste	122	283
Medien	4	7
Technik	4	8
Personenstandswesen	1	2
Statistik	1	1
Bau- und Vermessungswesen	3	1
Hochschulen	6	9
Scientology	5	5
Umweltschutz	2	0
Sonstiges, öff.	15	7
Eingaben insgesamt[3]	867	1115

[3] Aufgrund der statistischen Erhebungsmethode weicht die rechnerische Summe von der angegebenen Zahl ab. Ab 2010 wird ein neues statistisches Zählverfahren eingeführt, das einen übereinstimmenden Wert ergibt.

Die nachfolgenden Übersichten der vergangenen 10 Jahre verdeutlichen den Anstieg der Eingaben insgesamt und stellen zudem den steigenden Anteil der Eingaben im nicht-öffentlichen Bereich dar:

Jahr	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
Summe aller Eingaben	509	610	562	542	569	647	643	690	867	1115
Versicherungswirtschaft	21	21	22	21	37	26	19	19	29	27
Kreditwirtschaft	15	38	25	21	12	24	15	33	31	38
Priv. Wohnungswirtschaft	16	11	9	16	14	18	6	16	16	22
Versandhandel	9	7	8	10	11	8	9	15	22	18
sonst. Handel	11	19	17	20	20	32	22	33	46	58
Werbung, Direktmarketing	51	79	103	80	86	116	84	107	158	163
Schufa, Auskunfteien	40	47	42	53	35	40	35	53	50	45
Markt- und Meinungsforschung	3	5	1	2	1	10	1	7	7	13
Vereine, Parteien	5	7	9	11	8	11	21	9	12	20
Freie Berufe	4	6	2	20	45	15	12	22	33	54
Soziales u. Gesundheitsw., nicht-öff.	21	19	14	19	14	18	13	4	20	21
Personal/DS, nicht-öff.	20	20	28	21	13	18	24	22	24	31
Verkehrswesen, nicht-öff.	9	5	14	2	6	3	2	3	9	11
Sonstiges, nicht-öff.	40	28	24	25	14	42	55	48	49	50
Telekommunikation	7	15	11	11	19	15	24	10	10	32
Tele- und Mediendienste	46	78	87	43	44	36	39	51	122	283
Medien	6	5	3	6	3	7	2	7	4	7
Nicht-öffentlich gesamt	324	411	419	389	383	439	393	459	643	893
Anteil nicht-öffentlich an Gesamtzahl in %	**64**	**67**	**75**	**72**	**67**	**68**	**61**	**67**	**74**	**80**

V. INFORMATIONSFREIHEIT

1. Leitbild und Ziele

1.1 Kooperation und Dialog haben Priorität

Unser Ziel ist es, die Hamburgische Verwaltung einschließlich der Institutionen der mittelbaren Staatsverwaltung und der Beliehenen bei der Entwicklung einer Kultur der Informationsfreundlichkeit zu unterstützen. Damit jedoch unsere Hinweise und Ratschläge auch im Falle risikobehafteter Entscheidungen bei den Anwenderinnen und Anwendern auf fruchtbaren Boden fallen, müssen diese möglichst praxisnah und fachspezifisch erteilt werden. Um maßgeschneiderte Hilfen anbieten zu können, müssen wir die einzelnen Fachmaterien und die administrativen Rahmenbedingungen kennen und auf dieser Basis mit den Anwenderinnen und Anwendern in Dialog treten.

Es geht darum, den entscheidenden Rechtsgrundsätzen bei der Anwendung des HmbIFG Geltung zu verleihen und zugleich die Verwaltung zu motivieren, auch für komplexere Anträge auf Informationszugang informationsfreiheitsfreundliche Lösungen zu finden. Was bedeutet es zum Beispiel im Lichte der Maxime, wonach Ausnahmen von der Informationsfreiheit eng auszulegen sind, Bürgerinnen und Bürgern das Argument entgegenzuhalten, ihr Informationszugang verbiete sich wegen unverhältnismäßigen Verwaltungsaufwands? Hier sind flexible Vorgehensweisen gefragt, die ohne Einbußen für die Informationszugang Beantragenden den Verwaltungsaufwand möglichst gering halten. Die richtigen Schritte und Methoden sind anhand der im Informationsfreiheitsrecht vorgezeichneten Leitlinien in Abstimmung mit der Praxis zu entwickeln. Wir setzen hier auf Kommunikation und Kooperation mit den informationspflichtigen Behörden, damit diese sich die Maßstäbe und Standards der Informationsfreiheit in der Praxis effektiv zu Eigen machen.

Der HmbBfDI ist, ebenso wie als Verantwortlicher für den Datenschutz, auch im Bereich der Informationsfreiheit seiner Rechtsstellung nach unabhängig. Daher erfolgt unsere Meinungs- und Überzeugungsbildung unabhängig von äußerer Einflussnahme. Der Meinungsbildungsprozess ist gleichwohl ein offener und integrativer, da gerade die Informationsfreiheit ihrem demokratischen Anspruch nach nicht verordnet, sondern zivilgesellschaftlich angeeignet werden soll. Zu unserem Aufgabenverständnis gehört es, auch und gerade auf dem Gebiet der Informationsfreiheit ein gut vernetzter Katalysator im Wissenstransfer zu sein. Die Vorteile liegen auf der Hand:

- Im Dialog mit uns gewinnen die Behörden Sicherheit bei der Anwendung informationsfreiheitsrechtlicher Vorschriften,
- die Erfahrungen der einzelnen Anwendungsbereiche können ausgetauscht und übergreifend nutzbar gemacht werden,
- durch Kooperation insbesondere mit der federführenden Justizbehörde lassen sich informationsfreundliche Maßstäbe fortlaufend weiterentwickeln,
- ein gemeinsames Ringen um best-practice fördert die Transparenz staatlichen Handelns und dient – nicht zuletzt -
- dem Interesse der Allgemeinheit an einer wirksamen und rechtssicheren Handhabung des Informationszugangs.

1.2 Information geht vor Kritik

Nach unserem Verständnis und – erfreulicher Weise auch nach unseren bisherigen Erfahrungen – sind behördliche Stellen weitestgehend bestrebt, sich rasch mit der noch relativ neuen Materie der Informationsfreiheit vertraut zu machen, um auf gesicherter rechtlicher Basis einen servicefreundlichen Zugang zu ihren amtlichen Informationen zu eröffnen.

Da allerdings zu dem neuen HmbIFG noch kaum Rechtsprechung vorliegt und auf der Grundlage von Informationsfreiheitsgesetzen des Bundes und anderer Länder ergangene gerichtliche Entscheidungen nur annäherungsweise herangezogen werden können, steht die Praxis noch vor vielen offenen Fragen. Hier kommt es entscheidend darauf an, die Behörden durch fachkompetente Informationsangebote zu ertüchtigen. Wir legen daher das Schwergewicht unserer Aktivitäten auf die Schulung, Fortbildung und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter der Verwaltung und sonstiger zum Anwendungsbereich des HmbIFG gehörender Stellen. Auch Einzelgespräche und telefonische Beratungen gehören zu unseren Angeboten.

Wir sehen unsere Aufgabe darin, auf eine informationsfreiheitsfreundliche Auslegung des HmbIFG hinzuwirken. Eine solche Auslegungspraxis kann sich dabei erst dann zum Maßstab verfestigen, wenn sie sich nicht allein vom Ziel her, sondern auch im Ergebnis informationsfreiheitsfreundlich bewährt hat. Hier dürften auch in technisch-organisatorischer Hinsicht noch manche Fragen auftauchen und einvernehmlich zu klären sein. Vor diesem Hintergrund sollte auf den Einsatz von beanstandender Kritik behördlichen Handelns weitestgehend verzichtet werden. Wir beabsichtigen nicht, uns von Vornherein der Möglichkeit zu begeben, gänzlich von Kritik abzusehen. Verdeutlicht werden soll vielmehr, dass nach dem Grundsatz der Verhältnismäßigkeit Kritik erst dort einsetzen soll, wo die milderen Formen des Dialogs und der Beratung nicht den gewünschten Erfolg erzielt haben.

1.3 Beratung geht vor Beanstandung

Stellt der HmbBfDI Verstöße gegen das HmbIFG bei den zum Anwendungsbereich dieses Gesetzes gehörenden Stellen fest, so fordert er sie zur Mängelbeseitigung auf. Bei erheblichen Verletzungen des Informationsfreiheitsrechts beanstandet der HmbBfDI dies bei den verantwortlichen Leitungs- oder Aufsichtsorganen (§ 15 Abs. 5 HmbIFG).

Uns ist damit im Bereich der Informationsfreiheit das gleiche Instrumentarium an die Hand gegeben wie im Bereich des Datenschutzes. In dem relativ kurzen Zeitraum der Berichterstattung ist es im Bereich der Informationsfreiheit nicht zu förmlichen Beanstandungen gekommen. Eine Prognose für die weitere Zukunft ist daraus nicht abzuleiten; wir arbeiten jedoch wie Eingangs dargestellt daraufhin, die Behörden und sonstigen informationszugangsverpflichteten Stellen dahingehend zu ermutigen, unsere Beratungskompetenz wie auch die Vernetzungsstrukturen der Behörden untereinander zu nutzen, um zu einer rationalen und transparenten Praxis der Rechtsanwendung zu gelangen.

2. Handlungsfelder

2.1 Öffentlichkeitsarbeit

Im Bereich der Informationsfreiheit zielt unsere Öffentlichkeitsarbeit darauf, die Bevölkerung breitenwirksam und effektiv auf das neue Informationsfreiheitsrecht und die Angebote unserer Dienststelle aufmerksam zu machen. Als ersten Schritt haben wir einen handlichen Flyer zum Thema Informationsfreiheit herausgegeben und in Papierform über die Hamburgischen Behörden und Dienststellen der Öffentlichkeit zur Verfügung gestellt. Der Flyer kann zudem über unsere Geschäftsstelle bezogen und als Pdf-Datei von unserer Homepage heruntergeladen werden. Mit dem Flyer möchten wir insbesondere jene Menschen erreichen, die bislang nicht mit dem Thema Informationsfreiheit in Berührung gekommen sind.

Noch ist das Wissen über das demokratische Teilhaberecht Informationsfreiheit nicht allgemein im Bewusstsein der Öffentlichkeit verankert, wie dies vergleichsweise seit mehr als 25 Jahren beim Datenschutz der Fall ist. Ziel der Öffentlichkeitsarbeit ist es daher, die Bedeutung der Transparenz behördlichen Handelns in einer demokratischen Zivilgesellschaft zu verdeutlichen und die Bürgerinnen und Bürger zu ermuntern, uns in Fragen der Informationsfreiheit anzurufen. Unterstützt durch zielgerechte Öffentlichkeitsarbeit soll unsere Dienststelle auch auf dem Gebiet der Informationsfreiheit zu einer bekannten Institution werden, an die sich Bürgerinnen und Bürger gern wenden, wenn ihnen der Zugang zu behördlichen Informationen verwehrt, nicht zeitgerecht oder nur unzulänglich erteilt wurde.

2.2 Behördlicher Arbeitskreis

Bei der ministeriell federführenden Justizbehörde besteht ein Arbeitskreis der Informationsreferentinnen und Informationsreferenten der einzelnen Behörden und Dienststellen. In diesem Arbeitskreis ist auch unsere Dienststelle vertreten. Nachdem sich die Angehörigen des Referats Informationsfreiheit bereits an schriftlichen Abstimmungsprozessen beteiligt hatten, nehmen sie seit Oktober 2009 an dessen Sitzungen teil. Wir haben bereits die aus dem Arbeitskreis geäußerte Anregung zur Überarbeitung der von der Justizbehörde herausgegebenen Anwendungshinweise aufgenommen und einen einheitlichen Neuentwurf in die Abstimmung im Arbeitskreis geben lassen. Der von uns erstellte Entwurf umfasst zugleich eine von ihm erstellte so genannte Checkliste für Anwenderinnen und Anwender des Hamburgischen Informationsfreiheitsgesetzes, um den Praktikerinnen und Praktikern vor Ort eine aktuelle und hilfreiche Handlungsanleitung für die Praxis der Informationsfreiheit zu geben.

2.3 Konferenz der IF-Beauftragten

Durch das neue, am 28. Februar 2009 in Kraft getretene HmbIFG ist in Hamburg erstmalig die Funktion eines Beauftragten für die Informationsfreiheit geschaffen worden. Nach § 15 Abs. 1 HmbIFG kann eine Person, die der Ansicht ist, dass ihr Informationsersuchen zu Unrecht abgelehnt oder nicht beachtet worden ist oder dass sie von der auskunftspflichtigen Stelle eine unzulängliche Auskunft erhalten hat, den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit anrufen.

Der Informationsfreiheitsbeauftragte des Bundes und die Informationsfreiheitsbeauftragten der Länder bilden die Konferenz der Informationsfreiheitsbeauftragten (IFK), der nunmehr auch der HmbBfDI in Person angehört. Als Neumitglied oblag

es ihm, im Jahre 2009 die 19. Konferenz dieses Gremiums sowie die vorbereitende Sitzung des Arbeitskreises der Referentinnen und Referenten für das Informationsfreiheitsrecht des Bundes und der Länder (AKIF) auszurichten. Im Anschluss an die im November 2009 durchgeführte AKIF-Sitzung fand die IFK am 16. Dezember 2009 in Hamburg, eingeleitet mit einem Grußwort von Justizsenator Herrn Dr. Steffen, statt. Dem Transparenzgedanken folgend, werden die Einladungen zu den Sitzungen des AKIF wie insbesondere auch der IFK im Internet veröffentlicht, um allen Bürgerinnen und Bürgern einen freien Zugang zu den – im gesamten Verlauf öffentlichen – Sitzungen zu ermöglichen. Auch die Beschlüsse der IFK sind im Internet abrufbar. Aus unserer Sicht bietet die IFK ein unverzichtbares Forum für einen Bund und Länder übergreifenden Meinungs- und Erfahrungsaustausch. Entsprechend groß ist unser Interesse an einer weiteren aktiven Mitwirkung.

2.4 Fortbildungsveranstaltungen

Wir haben auf der Ebene der Bezirksverwaltung auf Anfrage des Bezirksamtes Hamburg-Mitte mehrere Seminare, die sich in erster Linie an Angehörige der Bezirksverwaltung richteten, kostenfrei veranstaltet. Mit jeweils ca. 60 Teilnehmenden waren diese Veranstaltungen gut besucht und haben insbesondere dazu beigetragen, uns als Ansprechpartner für Fragen der Informationsfreiheit kennenzulernen. Umgekehrt haben wir derartige Veranstaltungen genutzt, um im Dialog mit den Teilnehmenden zu ermitteln, wo Schwerpunkte bei der praktischen Inanspruchnahme des Informationszugangsrechts erkennbar sind und welche rechtlichen und administrativen Spezialprobleme noch Fragen zur Auslegung und praktischen Handhabung des HmbIFG aufwerfen.

Insgesamt zielen derartige Seminare darauf ab, die im HmbIFG und im dazugehörigen Gebührenrecht angelegten Zielkonflikte für die Anwenderinnen und Anwender offen zu benennen und gleichzeitig Hinweise zu geben, wie diese Konflikte informationsfreiheitsfreundlich aufgelöst werden sollten. Die anforderungsgerechte Eröffnung von Informationszugang kann möglicherweise mit einem hohen Verwaltungsaufwand verbunden sein und wegen des gebührenrechtlichen Kostendeckungsprinzips dazu führen, dass entsprechend höhere Gebühren festzusetzen sind. Da gleichzeitig darauf zu achten ist, dass die Höhe der Gebühr keine Wirkung entfaltet, die von der Inanspruchnahme des Informationszugangs abschreckt, kann hierdurch ein Zielkonflikt entstehen. Ein weiterer denkbarer Zielkonflikt kann auftreten, wenn einerseits die auskunftspflichtige Stelle fristgerecht den Informationszugang eröffnen möchte, aber die Einholung von Einwilligungen Betroffener zur Offenbarung ihrer Daten längere Zeit in Anspruch nimmt.

Der Schlüssel zur Lösung derartiger Zielkonflikte ist die Beratung. Wir empfehlen den auskunftspflichtigen Stellen in diesem Sinne zunächst den Antragstellenden mitzuteilen, ob

- die gewünschten Informationen bei der auskunftspflichtigen Stelle vorhanden sind,
- angesichts von Schwierigkeit und Umfang mit relativ hohen Gebühren zu rechnen wäre.

Sodann sollte mit den Antragstellenden beratend erörtert werden, ob

- das Zugangsbegehren hinreichend präzise dargelegt ist,
- gegebenenfalls aus verwaltungspraktischen Gründen eine schriftliche Antragstellung angezeigt wäre,

- Auskunft, Einsichtnahme oder die Anfertigung von Kopien gewünscht wird,
- angesichts der Gebührenhöhe gegebenenfalls eine kostengünstigere Variante in Frage kommt.

Wir sind bestrebt, die auf die Anwendung des HmbIFG übertragbaren Hinweise aus der zu den Informationsfreiheits- und Informationszugangsgesetzen des Bundes und der Länder ergangenen Rechtsprechung in ein Schulungskonzept zu integrieren. Ebenso werden die eigenen Erfahrungen sowie die Erfahrungen der Behörden und Dienststellen mit dem neuen HmbIFG fortlaufend einbezogen. Künftig sind ganztägige Fortbildungsveranstaltungen beim Zentrum für Aus- und Fortbildung (ZAF) geplant.

2.5 Einzelfälle

In dem kurzen Zeitraum, den das neue HmbIFG gilt und wir zu seiner Durchsetzung angerufen werden können, kam es zu 19 schriftlichen Eingaben und rund 250 Anfragen, die telefonisch erfolgten und auch so erledigt wurden. Insgesamt hat sich gezeigt, dass Behörden dazu neigen, sich auf altbekannte Rechtsnormen zu berufen und das HmbIFG aufgrund der vermeintlich vorrangigen Spezialregelungen nach § 16 nicht anzuwenden. Diese Vorgehensweise ist insbesondere dann zu beobachten, wenn nach den bekannten Vorschriften ein Anspruch abgelehnt werden könnte. Eine Ursache für diese Vorgehensweise könnte in einer gewissen Unsicherheit im Bezug auf die Anwendung des HmbIFG bestehen. Aus Furcht, zu viele Informationen preiszugeben, wird der Anspruch eher in seiner Gesamtheit verneint. Als effektive Vorgehensweise hat es sich aus unserer Sicht hier bewährt, nicht mit Beanstandungen oder formellen Rügen zu arbeiten. Erfolg versprechender ist hier die Zusammenarbeit mit der verantwortlichen Stelle.

Beispielsfälle: Ein Bürger hat Auskunft von der JVA Fuhlsbüttel zu internen Richtlinien über die Gestaltung der Freizeit der Insassen begehrt. Während die Leitung der JVA Fuhlsbüttel einen Anspruch unter Verweis auf die nur vermeintlich vorrangigen §§ 127 StVollzG, 18 HmbDSG verneinte, schloss sich das Strafvollzugsamt der Justizbehörde unserer Auffassung an und erteilte die begehrte Auskunft.

Als sinnvoll hat sich die Einbeziehung der mittelbaren Staatsverwaltung nach § 3 Abs. 1 HmbIFG durch den Gesetzgeber erwiesen. Von Stellen der mittelbaren Staatsverwaltung, also Anstalten, Stiftungen und Körperschaften öffentlichen Rechts, haben Bürger häufig Auskunft begehrt. Dies betraf im Berichtszeitraum zum Beispiel die Kassenärztliche Vereinigung Hamburg, die Hamburgische Ärztekammer, die Medienanstalt Hamburg/Schleswig-Holstein und die Handelskammer Hamburg. Zu dem durch das neue HmbIFG erweiterten Anwendungsbereich ist anzumerken, dass auch Informationen, die beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit vorhanden sind, Gegenstand von Auskunftsverlangen waren.

Der Anspruch des HmbIFG gilt grundsätzlich auch für Bauakten. Probleme können sich hier ergeben, weil eine Anonymisierung unter Nachbarn oft nicht möglich ist. Da sich viele Beteiligte aufgrund des Nachbarschaftsverhältnisses untereinander kennen, kann eine Schwärzung der Unterlagen oft nicht den gleichen persönlichkeitsrechtsschützenden Effekt haben wie in anderen Konstellationen. Eine Ablehnung des Anspruchs aufgrund der bloßen Möglichkeit der Identifikation erscheint jedoch ebenso wenig vorzugswürdig. Nachbarschaftsstreitigkeiten sind häufig mit dem Umweltinformationsgesetz zu lösen. Dies ist eines der wenigen Gesetze, die

einen weiteren Anwendungsbereich haben als das Hamburgische Informationsfreiheitsgesetz.

Auch in streitigen Fällen konnte bisher bei Einschaltung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit immer ein Gerichtsverfahren vermieden werden. Streitige Fälle sind im Berichtszeitraum nicht über das Stadium eines Widerspruchsverfahrens hinaus gegangen.

Vereinzelt wurden Anträge mit der Begründung abgewiesen, bei den begehrten Informationen handele es sich lediglich um verwaltungsinterne Richtlinien ohne Bindungswirkung. Da diese nicht auf konkrete Fälle bezogen seien, unterlägen sie nicht der Definition der „vorhandenen Information" nach § 1 HmbIFG. Wir vertreten hier die Auffassung, dass grundsätzlich alle bei der auskunftspflichtigen Stelle vorhandenen Informationen dem HmbIFG unterliegen. Der Bezug zu einem konkreten Verwaltungsverfahren ist nicht erforderlich. Vielmehr kann die Herausgabe von begehrten Informationen nur dann unter Berufung auf § 3 Abs. 2 Nummer 6 HmbIFG verweigert werden, wenn es die gerichtliche oder außergerichtliche Geltendmachung oder Abwehr von Ansprüchen in einem konkreten Fall betrifft. In dem konkreten Fall wurde die begehrte Information dem Antragsteller aufgrund eines eingelegten Widerspruchs zur Verfügung gestellt.

In den Berichtszeitraum fielen auch Informationsansprüche von Bürgerinnen und Bürgern, die unter anderem Betriebs- und Geschäftsgeheimnisse zum Gegenstand hatten. Hier hat sich gezeigt, dass die Schwärzung und teilweise Herausgabe von Informationen einen tragfähigen Kompromiss zwischen dem Informationsinteresse der Bürger und dem nachvollziehbaren Interesse an Vertraulichkeit der Inhaber von Betriebs- und Geschäftsgeheimnissen darstellt. Insbesondere kann die konsequente Einhaltung des in § 14 HmbIFG statuierten Trennungsprinzips helfen, den bei der nur teilweisen Herausgabe erforderlichen Aufwand gering zu halten.

Der Schutz personenbezogener Daten stellte im Berichtszeitraum die größte Herausforderung dar. Vereinzelt haben Marketingunternehmen versucht, von Stellen der mittelbaren Staatsverwaltung vollständige Listen von Freiberuflern zu erhalten. Da eine Begründung des Antrags nicht erforderlich ist, können keine definitiven Aussagen über die Motive gemacht werden. Es liegt jedoch die Vermutung nahe, dass es sich um die Durchführung von Marketingmaßnahmen handelte. Zwar ist die auskunftspflichtige Stelle grundsätzlich nach § 12 HmbIFG gehalten, die Betroffenen um Einwilligung in die Freigabe der begehrten Information zu ersuchen. Dies bedeutet jedoch nicht, dass bei jedem Mitglied aufgrund jedes Antrags erneut um Einwilligung ersucht werden muss. Dies gilt insbesondere, da es sich bei der Anfrage nach einer vollständigen Liste der personenbezogenen Daten aller Mitglieder um einen Ausforschungsantrag handelt. Diesem muss nicht entsprochen werden, wie sich schon aus der Gesetzesbegründung zu § 11 Nr. 4 HmbIFG ergibt.

Grundsätzlich anders gelagert sind Fälle, in denen Auskunft über die Identität bestimmter Personen verlangt wird, soweit diese in amtlicher Funktion tätig werden. So begehrte eine Antragstellerin Auskunft über die Identität von Prüfern einer in Kürze stattfindenden Prüfung zum Abschluss ihrer Ausbildung. Diesem Antrag war stattzugeben, da der Prüfling eine Besorgnis der Befangenheit des Prüfers geltend machte, die durch Bekanntgabe der Identität behoben werden konnte. Bei der vorzunehmenden Abwägung war insbesondere zu berücksichtigen, dass die Identitäten der Prüfer im Rahmen der kurze Zeit später stattfindenden Prüfung ohnehin offenbart worden wären. Hier zeigte sich auch, dass Informationsbegehren bisweilen

unter Berufung auf „Datenschutzgründe" abgelehnt werden, ohne dass überhaupt eine Abwägung stattfindet.

Im Vergaberecht kommt es regelmäßig zu vermeintlichen Kollisionen von Ansprüchen nach dem HmbIFG und denen nach § 111 GWB. Die Lösung ist hier, dass die Ansprüche nach dem Gesetz gegen Wettbewerbsbeschränkungen gemäß § 100 Abs. 1 GWB nur dann einschlägig sind, und auch nur dann die Ansprüche nach dem HmbIFG verdrängen können, wenn der Schwellenwert überschritten wird, der nach einer aufgrund von § 127 GWB erlassenen Rechtsverordnung festgelegt wird. Bestehen Ansprüche nach dem HmbIFG in einem Vergabeverfahren, so sind hier häufig auch Betriebs- und Geschäftsgeheimnisse der Teilnehmer an einem solchen Verfahren betroffen. Der Auftragswert als solcher enthält keine schützenswerten Betriebs- und Geschäftsgeheimnisse, da aus diesem allein keine Rückschlüsse auf die geschäftliche Situation der Teilnehmer gezogen werden können. Dies gilt aber nicht, soweit Informationen über die Preiskalkulation betroffen sind. Eine Offenbarung von Informationen über die Kalkulation würde Wettbewerbern Einblick in die Kosten- und Personalstrukturen von Auftragnehmern ermöglichen und wäre so geeignet, deren Stellung im Wettbewerb negativ zu beeinflussen. Bei einer Beeinträchtigung von Betriebs- oder Geschäftsgeheimnissen ist nach § 10 Abs. 1 HmbIFG eine Abwägung zwischen den schutzwürdigen Belangen des Betroffenen und dem Offenbarungsinteresse der Allgemeinheit vorzunehmen. Nach dem Willen des Gesetzgebers führt dies aufgrund des grundrechtlichen Schutzes von Betriebs- und Geschäftsgeheimnissen nach Art. 12, 14 GG regelmäßig zu einem Überwiegen des Geheimhaltungsinteresses. Ein sinnvoller Ausgleich zwischen beiden Interessen kann gefunden werden, indem die Teile der behördlichen Aufzeichnungen, die Betriebs- und Geschäftsgeheimnisse enthalten, geschwärzt werden, während die Teile, die nicht den Schutz von § 10 HmbIFG genießen, an den Antragsteller herausgegeben werden. In den in den Berichtszeitraum liegenden Fällen sind Hamburger Behörden wie beschrieben verfahren.

Hamburger Behörden haben von der Möglichkeit, Gebühren zu erheben, in erfreulich zurückhaltender Weise Gebrauch gemacht. Dem Grundgedanken des HmbIFG folgend, sind keine Fälle bekannt, in denen Gebühren erhoben wurden, die eine abschreckende Wirkung gehabt hätten oder geeignet gewesen wären, Bürgerinnen und Bürger von der Geltendmachung informationsfreiheitsrechtlicher Ansprüche abzuhalten.

2.6 Beobachtung der Rechtsprechungslandschaft

Die Rechtsprechung ist grundsätzlich informationsfreiheitsfreundlich.

Da es sich bei der Informationsfreiheit, zumindest aus Hamburger Sicht, um ein junges Rechtsgebiet handelt, existiert hierzu noch wenig Rechtsprechung. Die bisher erschienenen wissenschaftlichen Veröffentlichungen bewegen sich daher noch auf juristisch wenig erschlossenem Gelände. Umso größere Bedeutung hat die Beobachtung und Auswertung der zur Informationsfreiheit ergangenen Rechtsprechung in den einschlägigen Fachzeitschriften, der Tagespresse und den elektronischen Veröffentlichungen.

Grundsätzlich lässt sich sagen, dass es sich bei den Fällen, die bis zu einer Klage getrieben wurden, um Fälle handelt, denen ein hohes Gewicht zukommt. Dabei handelt es sich häufig um Auskunftsansprüche, die aus beruflichen Gründen von Journalisten oder Rechtsanwälten geltend gemacht werden.

Eines der größten Probleme ist nach wie vor die Konkurrenz verschiedener Auskunftsansprüche. Dies betrifft Ansprüche nach dem hamburgischen Umweltinformationsgesetz, dem Verbraucherinformationsgesetz und einer Vielzahl weiterer Spezialgesetze sowie Ansprüche auf Akteneinsicht im Verwaltungsverfahren. Leider existiert hierzu bisher nur relativ wenig Rechtsprechung. Dadurch sind die Urteile kaum dazu geeignet, die aufgeworfenen Probleme abschließend zu beantworten. Ein Urteil aus Neustadt (an der Weinstraße) macht jedoch Vorgaben, die als Auslegungshilfe herangezogen werden können. Danach sind Auskunftsnormen grundsätzlich nebeneinander anzuwenden. Eine Verdrängung durch Spezialität liegt nur dann vor, wenn ein umfassender Informationsanspruch, wie er nach dem IFG besteht, dem Schutzzweck des Spezialgesetzes zuwiderlaufen würde. Dies ist zum Beispiel bei Ansprüchen nach den Landespressegesetzen nicht der Fall.

Insgesamt lässt die Rechtsprechung eine positive Einstellung zur Informationsfreiheit erkennen. Die Ausnahmetatbestände sind auf die gesetzlich normierten zu begrenzen und grundsätzlich eng auszulegen. Eine wichtige Rolle spielt dabei insgesamt der aus Grundrechten abgeleitete Schutz von Betriebs- und Geschäftsgeheimnissen.

Nach der Rechtsprechung steht der Informationsanspruch auch Amtsträgern zu, und zwar sogar dann, wenn sie ihn in ihrer Eigenschaft als Amtsträger geltend machen. Die durch das Hamburgische Informationsfreiheitsgesetz bewirkte Öffnung des Informationszugangs für jedermann bewirkt, dass die in der Rechtsprechung verschiedentlich erörterte „Strohmann"-Problematik entfällt.

Das Bundesverwaltungsgericht hat entschieden, dass die formale Einstufung einer Information als „Verschlusssache – Nur für den Dienstgebrauch" einen Anspruch auf Informationszugang nach dem Informationsfreiheitsgesetz nicht automatisch ausschließe. Die Verwaltungsgerichte hätten vielmehr zu prüfen, ob die konkreten Informationen tatsächlich so beschaffen seien, dass die Kenntnisnahme durch die Öffentlichkeit für die Interessen der Bundesrepublik nachteilig sein könnte. In einer weiteren Entscheidung vom gleichen Tag ging das Bundesverwaltungsgericht jedoch davon aus, dass der Regierung bei der Außenpolitik ein weitgesteckter Spielraum zusteht, der sowohl die außenpolitischen Ziele umfasst als auch die Frage, wie diese zu erreichen seien. Nur mit Blick auf diese Ziele könne eingeschätzt werden, ob das Bekanntwerden einer Information Nachteile für die internationalen Beziehungen bedeute oder nicht. Dies umfasse darüber hinaus auch eine Prognose, die ihrerseits nur in engen Grenzen verwaltungsgerichtlich überprüfbar sei. Daher sei ein Anspruch auf Informationszugang abzulehnen, wenn die Regierung nachteilige Auswirkungen auf die internationalen Beziehungen befürchte. Auch wenn die praktische Relevanz für Hamburg vermutlich gering sein wird, so handelt es sich doch um Tendenzen in der Rechtsprechung, die es weiter zu beobachten gilt.

2.7 Erstellung von Rechtsgutachten

Bürgerschaft und Senat sind jeweils in ihrer eigenen Sphäre für den Geheimnisschutz verantwortlich.

Zu unserer Aufgabe gehört nach § 15 Abs. 4 Satz 4 HmbIFG auch das Erstellen von Rechtsgutachten auf Anforderung der Bürgerschaft oder des Senats. Dies ist im kurzen Geltungszeitraum von § 15 Abs. 4 Satz 4 HmbIFG während des Berichtszeitraums noch nicht vorgekommen. Es sind allerdings Fälle behandelt worden, die

über den Einzelfall hinaus Auswirkungen auf die behördliche Praxis haben, auch wenn die Voraussetzungen des § 15 Abs. 4 Satz 4 HmbIFG nicht vorgelegen haben.

In einem solchen Fall ging es um das Verhältnis der Bürgerschaft zum Senat und die Frage, wer für den Geheimnisschutz zuständig ist. Wir gelangten zu der Ansicht, dass Senat und Bürgerschaft ihre Geheimnissphären jeweils eigenverantwortlich für ihren Bereich zu schützen haben. Der Senat hat die Vorkehrungen der Bürgerschaft zum Geheimnisschutz lediglich von außen her zu respektieren, wie umgekehrt die Bürgerschaft die durch Gesetz und Verfassung geschützten Geheimnissphären des Senats zu achten hat. Beim Schutz der Geheimnissphären des Senats ist insbesondere der Kernbereich exekutiver Willensbildung zu berücksichtigen.

3. Eine erste Bilanz

3.1 Möglichkeiten und Grenzen der Hilfe durch den HmbBfDI

Der HmbBfDI kann nach § 15 HmbIFG im Bereich der Informationsfreiheit das gesamte Instrumentarium einsetzen, wie es ihm im Bereich des Datenschutzes (§ 23 HmbDSG) zur Verfügung steht, um das Jedermann zustehende Recht auf Informationsfreiheit zu gewährleisten. Voraussetzung für eine wirksame Aufgabenwahrnehmung ist, dass

- die Bürgerinnen und Bürger ihr Recht auf Informationsfreiheit kennen und von ihm Gebrauch machen,
- die auskunftspflichtigen Stellen informationsfreiheitsfreundlich handeln,
- wir in Konflikt- und Zweifelsfällen möglichst frühzeitig beteiligt werden.

Hier zeigen sich bereits positive Ansätze, die es weiterzuverfolgen gilt. Zu bedenken ist, dass der voraussetzungslose Zugang zu amtlichen Informationen nicht schrankenlos ist. Die Grenzen der Informationsfreiheit sind als Ergebnis einer vom Gesetzgeber getroffenen Abwägung bereits im Gesetz enthalten und setzen somit auch unserem Bemühen um eine möglichst weitgehende Gewährleistung der Informationsfreiheit Grenzen.

Wir setzen daher unseren Schwerpunkt auf

- Information und Beratung,
- eine informationsfreiheitsfreundliche Auslegung des HmbIFG und
- die Schaffung einer informationsfreiheitsfreundlichen Verwaltungskultur.

Die Schaffung einer informationsfreiheitsfreundlichen Verwaltungskultur braucht mehr als guten Willen. Vielmehr müssen die behördlichen Stellen sich insgesamt informationsfreundlich aufstellen. Hierzu gehört insbesondere die Generierung, Pflege und Erschließung des Bestandes an amtlichen Aufzeichnungen mit den darin enthaltenen Informationen.

Was nicht in den Akten ist, existiert nicht in der Welt. Dieser seit dem Mittelalter anerkannte Grundsatz besitzt, nunmehr abgeleitet aus dem Rechtsstaatsprinzip, noch heute Geltung. Schriftgutverwaltung dient insbesondere im Verhältnis zu den Bürgerinnen und Bürgern den Erfordernissen des Verwaltungsverfahrensrechts, erfüllt darüber hinaus aber auch einige weitere wichtige Funktionen.

Aus Sicht der Informationsfreiheit ist zunächst von Bedeutung, dass in amtlichen Aufzeichnungen Informationen als „wertvolle Ressource" eingeschlossen sind.

Über den darin enthaltenen Nützlichkeitsaspekt hinaus gewährleistet die Schriftgutverwaltung die permanente Rechenschaftsfähigkeit der Organisation. Waren typischerweise bisher allein Prüfinstanzen wie Rechnungshof, Gerichte, das Parlament und dessen Untersuchungsausschüsse hierauf angewiesen, so fordert nunmehr auch die Informationsfreiheit eine rechenschaftsfähige Organisation für die Wahrnehmung des Rechts auf freien Zugang zu den bei Behörden vorhandenen amtlichen Informationen.

Konkret setzt die Wahrnehmung des Rechts auf freien Zugang zu behördlichen Informationen unabdingbar voraus, dass durch die Schriftgutverwaltung

- amtliche Informationen vollständig dokumentiert und aufbewahrt werden (Vollständigkeit),
- Bearbeiterinnen und Bearbeiter autorisiert und identifizierbar und Unbefugte ausgeschlossen sind (Authentizität),
- Tatsachen präzise, glaubhaft und überprüfbar wiederzugeben sind (Zuverlässigkeit),
- das Schriftgut nach seiner Erstellung gegen unbefugte Änderungen geschützt ist (Integrität) und
- Schriftgut nachgewiesen, auffindbar, darstellbar und verständlich ist (Benutzbarkeit).

(Vgl. Mummenthey/Kotte/Brüdegam, Selbstverständnis des Staatsarchivs Hamburg in einer modernen Verwaltung in: Information Wissenschaft und Praxis; 6-7/2009, S. 369, 376).

Für die Informationszugang suchenden Bürgerinnen und Bürger ist somit über die Tatsache hinaus, dass Informationen überhaupt in Akten (oder sonstigen Speichermedien) aufgezeichnet sind, von Bedeutung, dass die Informationen den oben genannten Anforderungen gerecht werden, um auch im Lichte der Informationsfreiheit ihren Zweck zu erfüllen. Schließlich wäre die bedeutendste Information wertlos, wenn sie zwar vorhanden, aber von mangelnder dokumentarischer Qualität oder schlicht nicht auffindbar wäre.

Daraus ergibt sich der Appell an die dem Anwendungsbereich des HmbIFG unterliegenden behördlichen Stellen, ihre Registraturen und Schriftgutverwaltungen, sei es in elektronischer, sei es in traditioneller Form, ordnungsgemäß und effizient zu führen, um damit die wichtigste Voraussetzung für einen effektiven Informationszugang zu sichern.

3.2 Stand des Erreichten

Das im Bereich der Informationsfreiheit bisher Erreichte kann nur die ersten Schritte auf dem Weg zu einer transparenten Verwaltung darstellen.

Die Aufgabe des Beauftragten für Informationsfreiheit fiel dem HmbBfDI nur für wenige Monate während des Berichtszeitraums zu. Dieser Tätigkeitsbericht kann daher nur Anfänge der Arbeit des Beauftragten auf dem Gebiet der Informationsfreiheit dokumentieren. Diese war geprägt durch eine Mischung aus der Bearbeitung von Einzelfällen von Petenten und der allgemeinen aufklärenden Arbeit zum Recht der Informationsfreiheit. Grundlegend bestehen hier große Überschneidungen zum Datenschutz. Aufgrund der Tatsache, dass es sich bei der Informationsfreiheit zumindest in Hamburg noch um ein im Vergleich zum Datenschutzrecht junges Rechtsgebiet handelt, lag der Schwerpunkt auf der allgemeinen aufklärenden Ar-

beit zum Recht der Informationsfreiheit. Dies betraf sowohl die Bürgerinnen und Bürger, die ermutigt werden sollen, von ihrem Recht Gebrauch zu machen, als auch die Behördenmitarbeiterinnen und Behördenmitarbeiter, denen Sicherheit im Umgang mit diesem jungen Rechtsgebiet gegeben werden soll.

Im Berichtszeitraum haben wir in einer juristischen Fachzeitschrift einen Artikel zum novellierten Hamburgischen Informationsfreiheitsgesetz veröffentlicht. Als jüngstem Mitglied in der Riege der Informationsfreiheitsbeauftragten des Bundes und der Länder oblag uns auch die Ausrichtung der beiden überregionalen Arbeitskreise: Dem Arbeitskreis Informationsfreiheit, in welchem sich die Referenten treffen, und der Konferenz der Informationsfreiheitsbeauftragten. Beide Veranstaltungen wurden während des Berichtszeitraums in Hamburg organisiert und erfolgreich veranstaltet. Die Intensivierung der Zusammenarbeit mit den Kolleginnen und Kollegen aus anderen Bundesländern und vom Bund hat sich dabei fachlich als sehr fruchtbar erwiesen. Dies gilt insbesondere für die Zusammenarbeit mit den Beauftragten, die bereits über eine größere Erfahrung auf dem Gebiet der Informationsfreiheit verfügen.

Zusammenfassend lässt sich sagen, dass die bisherige Arbeit nur die ersten Schritte auf einem langen Weg sein können. Am Ende des Weges werden aufgeklärte Bürgerinnen und Bürger stehen, die selbstbewusst von ihrem Recht auf Informationsfreiheit Gebrauch machen und dabei von den Behörden unterstützt werden. Durch den Erlass einer Vollregelung des Informationsfreiheitsgesetzes und der Erweiterung des Amtes des Datenschutzbeauftragten auf die Informationsfreiheit hat die Freie und Hansestadt Hamburg die ersten Schritte auf dem Weg zu einer transparenten Verwaltung gemacht. Wir werden dabei auch in Zukunft sowohl Bürgerinnen und Bürger als auch die Behörden unterstützen.

3.3 Ausblick

Informationsfreiheit durch Rechtssicherheit stärken.

Durch die Neufassung des HmbIFG vom 17. Februar 2009 wurde unsere Dienststelle als Garant für die Umsetzung dieses Gesetzes geschaffen. Bereits in diesem kurzen Zeitraum ist deutlich geworden, dass zwar der Zugang zu amtlichen Aufzeichnungen in rechtlicher Hinsicht ein voraussetzungsloser ist, die tatsächlichen Voraussetzungen für die Inanspruchnahme der Informationsfreiheit jedoch keineswegs automatisch gegeben sind. Um das Recht auf Informationszugang mit Leben zu erfüllen, müssen die Bürgerinnen und Bürger von ihm Gebrauch machen. Hierfür ist wiederum erforderlich, dass die Bürgerinnen und Bürger von diesem Recht überhaupt Kenntnis erlangen.

Die Kenntnis des Informationsfreiheitsrechts gilt es auch auf Seiten der Verwaltung zu vertiefen. Wir möchten auch innerhalb der Verwaltung das Bewusstsein dafür schärfen, dass sich das neue Recht nicht gegen die Verwaltung richtet, sondern Teil einer lebendigen Demokratie ist. Erfahrungen aus anderen Staaten zeigen, dass die Verwaltung die durch die Informationsfreiheit geschaffene Transparenz nicht zu fürchten braucht. Transparenz ist schließlich auch für die Verwaltung selbst von Vorteil, indem hierdurch Korruption und Selbstbegünstigung vorgebeugt wird. Nicht zuletzt dient eine transparente Verwaltung auch dem Abbau von Misstrauen und Vorbehalten gegenüber behördlichem Handeln.

Unsere Anstrengungen werden daher auch künftig darauf gerichtet sein, Bedingungen zu schaffen, in denen die Informationsfreiheit gedeihen kann. Eine wesent-

liche Bedingung ist die Schaffung von Rechtssicherheit. Nach den Erfahrungen beim Bund und in anderen Ländern setzen wir darauf, dass die Entwicklung einer informationsfreiheitsfreundlichen behördlichen Praxis durch die Gerichte konturiert und gefestigt wird. Schließlich müssen sowohl Bürger als auch Verwaltung in die Lage versetzt werden, verlässlich abschätzen zu können, welche Informationen herausgegeben werden und welche nicht. Eine besondere Bedeutung kommt dabei der sicheren Einschätzung der Gebührenfolge in jedem Einzelfall zu. Auch insoweit muss sowohl für Bürgerinnen und Bürger als auch für die Verwaltung Rechtssicherheit bestehen. Zusammenfassend ist festzustellen, dass wir in den nächsten Jahren vor der Herausforderung stehen, durch eine ebenso verlässliche wie informationsfreundliche Verwaltungspraxis die Kultur der Transparenz behördlichen Handelns zu stärken.

Dienststelle (Stand: 1. Februar 2010)

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
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:	Prof. Dr. Johannes Caspar	-4041-
Stellvertreter:	[redacted]	-4049-
Vorzimmer:		-4040-

Geschäfts- und Verwaltungsangelegenheiten der Dienststelle
[redacted] -4043-

Informationsmaterial
[redacted] -4042-
-4040-
-4042-

IT-Leitung und IT-Planung, Internetangebot der Dienststelle
[redacted] -4044-

E-Government, Chipkarten, technisch-organisatorische Beratung und Prüfung
[redacted] -4053-

Betriebssysteme, Netzwerke, Verschlüsselungstechniken, Signatur, Biometrie, technisch-organisatorische Beratung und Prüfung
[redacted] -4054-

Dokumentenmanagement/Archivierung, Videoüberwachungstechnik, technisch-organisatorische Beratung und Prüfung
[redacted] -4055-

Betriebssysteme, Netzwerke, Standardsoftware, technisch-organisatorische Beratung und Prüfung, anlassfreie Unternehmensprüfung
[redacted] -4061-

Elektronischer Rechtsverkehr, technisch-organisatorische Beratung und Prüfung

[redacted] –4048–

SAP, anlassfreie Unternehmensprüfung

[redacted] –4045–

Informationsfreiheit, Grundsatzangelegenheiten

[redacted] –4062–

Informationsfreiheit, Modernisierung des Datenschutzrechts

[redacted] –4047–

Informationsfreiheit

[redacted] –4051–

Gesundheitswesen, Justiz, Staatsanwaltschaft, Verfassungsschutz, Strafvollzug, Bauen und Wohnen, Umwelt, Kultur, Forschung, Archivwesen, Dokumentenmanagement

[redacted] –4049–

Ausländerwesen, Wirtschaftsverwaltung, Gewerberecht, Hochschulwesen Straßenverkehrsverwaltung, Wahlen und Volksabstimmungen, Waffenrecht

[redacted] –4064–

Polizei, Feuerwehr, Rundfunk, Medien

[redacted] –4052–

Soziales, Schulwesen, Kinderbetreuung, Allgemeine Bezirksangelegenheiten, Kirchen

[redacted] –4050–

Statistik, Personenstandswesen, Meldewesen, Ausweis- und Passangelegenheiten, Finanz-, Steuer- und Rechnungswesen

[redacted] –4046–

Auskunfteien, SCHUFA, Internationaler Datenverkehr, Bauen und Wohnen, Tele- und Mediendienste, Gewerbliche Dienstleistungen, Freie Berufe

[redacted] -4058-

Versicherungswirtschaft, Kreditwirtschaft, Handel und Industrie, Vereine, Telekommunkation

[redacted] -4059-

Arbeitnehmerdatenschutz, Personalwesen, Adresshandel, Werbung, Markt- und Meinungsforschung

[redacted] -4060-

Stichwortverzeichnis