BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG
20. Wahlperiode

Drucksache 20/3570
16.03.12

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

An die
Präsidentin der Hamburgischen Bürgerschaft

Betr.: 23. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI)

Anliegend übersende ich Ihnen unseren 23. Tätigkeitsbericht Datenschutz* für den Berichtszeitraum 2010/2011. Wie bereits in meinem Schreiben vom 13. Dezember 2011 mitgeteilt, beabsichtigen wir, die Tätigkeitsberichte Datenschutz und Informationsfreiheit im jährlichen Wechsel getrennt voneinander vorzulegen. Wir versprechen uns davon, dass die Themen so eher die ihnen gebührende Aufmerksamkeit finden. Der Ihnen vorliegende Tätigkeitsbericht beschäftigt sich daher nur mit dem Datenschutz.

Trotz dieser Beschränkung auf ein Thema ist der aktuelle Tätigkeitsbericht Datenschutz wieder eine bunte Mischung aus fast allen Lebensbereichen. Obwohl sich das Interesse der Öffentlichkeit stark auf das Internet fokussiert, ist auch der Datenschutz in der öffentlichen Verwaltung nach wie vor ein zentrales Thema, nicht zuletzt aufgrund der fortschreitenden Automatisierung des Verwaltungshandelns.

Zusätzlich zum Tätigkeitsbericht überreiche ich Ihnen unsere Broschüre „Datenschutz: Fakten-Zahlen-Daten“*, die nicht nur die Eingaben beim HmbBfDI im Berichtszeitraum quantifiziert, sondern sie auch mengenmäßig und thematisch mit den Zahlen der vergangenen zehn Jahre vergleicht. Dies ist unseres Erachtens eine sinnvolle Ergänzung des Tätigkeitsberichts, da die Broschüre dokumentiert, welche datenschutzrechtlichen Themen die Bürgerinnen und Bürger als besonders wichtig empfinden.

Ich wünsche Ihnen eine interessante Lektüre.

Prof. Dr. Johannes Caspar

* Verteilt nur an die Abgeordneten der Bürgerschaft.

Anlage 1

23. Tätigkeitsbericht Datenschutz 2010/2011 – HmbBfDI

Kontakt

Herausgeber:
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6
20095 Hamburg
Tel.: 040/42854-4040 (Geschäftsstelle)
Fax: 040/42854-4000
E-Mail: mailbox@datenschutz.hamburg.de

Titelbild: Thomas Krenz
Druck: Lütcke & Wulff, Hamburg

23. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zugleich Tätigkeitsbericht der Aufsichtsbehörde für den nicht-öffentlichen Bereich 2010 / 2011

Prof. Dr. Johannes Caspar
(Redaktionsschluss: 31. Dezember 2011)

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: 1.300 Exemplare

Druck: Lütcke & Wulff, 22525 Hamburg

23. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zugleich Tätigkeitsbericht der Aufsichtsbehörde für den nicht-öffentlichen Bereich 2010 / 2011

INHALTSVERZEICHNIS

Vorwort

Datenschutz ist eine Querschnittsmaterie. Die Aufgabe, das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger effektiv zu schützen, erstreckt sich auf die gesamte Breite des öffentlichen und des privaten Lebens. Personenbezogene Daten werden immer mehr zu zentralen Ressourcen für Gesellschaft und Staat. Sie vermitteln ökonomisch nutzbares Wissen ebenso wie die Möglichkeit der sozialen Kontrolle, aber auch neue Formen der Kommunikation miteinander. Die Bereiche, in denen wir im Berichtszeitraum 2010–2011 tätig waren, erwiesen sich entsprechend als komplex und breit gefächert.

Der Tätigkeitsbericht erfasst naturgemäß nur einen selektiven Ausschnitt der wichtigsten von uns bearbeiteten Themen. Aber bereits die vorliegende Zusammenstellung zeigt: Die Aufgabe der Wahrung des informationellen Selbstbestimmungsrechts in den unterschiedlichsten Sachverhalten, die den Eingaben von betroffenen Bürgerinnen und Bürgern sowie den zu überprüfenden IT-Anwendungen wie auch diversen Internet-Diensten zugrunde liegen, fordert eine zunehmende Spezialisierung in rechtlicher und technischer Hinsicht auf allen Ebenen der Dienststelle. Es ist daher erfreulich, dass es auch in den letzten zwei Jahren gelungen ist, mit unterschiedlichen Maßnahmen bzw. Informations- und Beratungsangeboten der Dienststelle das Datenschutzniveau zu verbessern. Das Erreichte wird uns künftig Maßstab und Ansporn sein.

Gleichzeitig dokumentiert der Tätigkeitsbericht, dass es nach wie vor eine Reihe von Problemfeldern gibt, in denen der Datenschutz bislang noch nicht den Stellenwert hat, der ihm eigentlich zukommen sollte. Hier wird deutlich, wo künftig bei öffentlichen und privaten Stellen noch Nachbesserungsbedarf besteht. Insoweit hält der Rückblick in die Vergangenheit bereits auch einen Blick in die Zukunft der Arbeit der Dienststelle bereit.

Prof. Dr. Johannes Caspar

Februar 2012

I. Umsetzung des Konzepts Hamburger Datenschutz 2010 – Entwicklungslinien und Analysen

Anlässlich des 22. Tätigkeitsberichts 2008/2009 wurden drei zentrale Module für ein modernes Konzept des Datenschutzes (Konzept Hamburger Datenschutz 2010) entwickelt. Diese sind in den letzten beiden Jahren schrittweise umgesetzt und laufend fortgeschrieben worden. Im Folgenden soll die Arbeit der Dienststelle analysiert und die Praxistauglichkeit der neuen Maßnahmen bewertet werden, um deren Implementierungsprozess zu optimieren.

1. Behördliche Kontrollverantwortlichkeit in der digitalen Welt

Im Tätigkeitsbericht 2008/2009 wurden Zahl und Gegenstand datenschutzrechtlicher Eingaben, d.h. schriftliche Beschwerden durch Bürgerinnen und Bürger, als zentrale Indikatoren für die Arbeitslast unserer Dienststelle gewertet. Die Zahlen dokumentieren einen Paradigmenwechsel von der Gefahr eines Überwachungsstaats hin zu einer digitalen Überwachungsgesellschaft. Diese Tendenz hat sich im abgeschlossenen Berichtszeitraum im Wesentlichen bestätigt. Von 2010 bis 2011 hat sich die Erhöhung des Eingabevolumens mit Schwerpunkt im nicht-öffentlichen Bereich, insbesondere im Bereich der Telemedien, deutlich weiter fortgesetzt.[1)] Das Verhältnis zwischen Beschwerden gegen nicht-öffentliche und gegen öffentliche Stellen liegt im Berichtszeitraum im Wesentlichen unverändert bei ca. fünf zu eins, d.h. auf fünf Beschwerden gegen private Datenverarbeitung kommt eine Beschwerde gegen öffentliche Stellen.

Für diese Entwicklung sind hauptursächlich eine zunehmende Ökonomisierung personenbezogener Daten sowie die immer rasanteren technologischen Innovationszyklen verantwortlich. Daneben bleibt aber auch eine unübersehbare Erosion des Begriffs der Privatsphäre ursächlich, die sich vornehmlich durch ein sozio-kulturelles Ideal der Selbstinszenierung und durch die Technisierung zwischenmenschlicher Beziehungen dokumentiert.

Gerade die technische Entwicklung entfaltet dabei zusätzlich eine unter datenschutzrechtlichen Aspekten bedenkliche Dynamik zur Privatisierung

[1)] Im Jahr 2010 betrug der Umfang der Eingaben allein gegenüber Telemediendiensten 43 % aller an uns gerichteter Beschwerden. Dagegen nehmen sich die Eingaben gegenüber dem besonders eingriffsintensiven Bereich der Polizei mit etwas mehr als 1 % aller Befassungen schon fast exotisch aus. Hierbei ist jedoch für den Zeitraum 2010 die besonders hohe Zahl mit Blick auf Beschwerden gegenüber dem Internetdienst Google Street View zu berücksichtigen. Diesen „saisonalen Effekt“ einmal ausgeblendet, ist der Anteil der Telemedien am Gesamtaufkommen für 2011 gegenüber 2010 rückläufig.

von Überwachungstechnologien. Dies ermöglicht es, dass in besonderem Maße komplexe digitale Techniken, die vormals im Bereich staatlicher Verwaltung zum Einsatz kamen, durch technische Innovationen und geringe Erwerbskosten künftig gerade auch von privaten Endverbrauchern genutzt werden. Vor allem dokumentiert sich diese Entwicklung durch den flächendeckenden Einsatz von Videotechnologien in Bereichen privater Lebensgestaltung wie auch geschäftlicher Zwecksetzungen von der Immobilienwirtschaft bis hin zum Arbeitsverhältnis.

Der rasante Anstieg auf 1.700 schriftliche Bürgerbeschwerden in 2010 – im Vergleich zur Situation vor 10 Jahren immerhin mehr als eine Verdreifachung – ist in erster Linie auf die bei der Behörde bundesweit eingegangenen Beschwerden gegen den Panoramadienst Google Street View zurückzuführen. Dennoch kann die Steigerung nicht lediglich auf dieses Einzelphänomen zurückgeführt werden. So ist im Verlauf von 2011 die Zahl der Eingaben gegenüber der bisherigen Spitze aus 2009 (1.115[2)]) noch einmal auf 1300 angestiegen. Sie befindet sich bei Herausrechnung der Eingaben gegen den Panoramadienst Google Street View auf ihrem bislang höchsten Niveau.[3)]

Als beunruhigend erweisen sich vor allem die Beschwerden gegenüber dem bundesweit agierenden sozialen Netzwerk Facebook mit ca. 20 Millionen Nutzern deutschlandweit, das seit Anfang 2010 eine Hauptniederlassung in Hamburg hat. Derzeit ist nicht absehbar, wie sich die Zahl der bundesweiten Eingaben entwickeln wird. Bereits heute bleibt festzustellen, dass der Aufgabenzuwachs, der aus der aufsichtsbehördlichen Kontrolle des weltweit größten sozialen Netzwerks erwächst, mit den derzeitigen personellen und finanziellen Ressourcen nur schwer sicherzustellen ist.

Die Kontrolle von international agierenden Internet-Konzernen, die mit verschiedenen Diensten (Gesichtserkennung, Freunde-Finder, Panorama-Bilder etc.) Daten von Nutzern sowie auch von unbeteiligten Dritten sammeln, werfen grundsätzliche Fragen auf, deren Beantwortung von zentraler Bedeutung für die Datenschutzaufsicht ist. Längst geht es nicht nur um die Frage der Beachtung des materiell-rechtlich Zulässigen, sondern darum, ob die angebotenen Dienste überhaupt im Anwendungsbereich europäischer bzw. nationaler Datenschutzvorschriften liegen und für deren Überwachung die Zuständigkeit deutscher Datenschutzbehörden gegeben ist.[4)]

[2)] Dazu TB 2008/2009, S. 132.

[3)] Zur Statistik, s. unter IV. 13.

[4)] Zur Zuständigkeit der Dienststelle s. unter IV.3.1.

Gegenwärtig ist festzuhalten, dass die Geltung des Datenschutzrechts in einer digital vernetzten Welt unklare Verantwortungszuschreibungen aufweist, die in erheblicher Weise gerade zu Lasten der informationellen Selbstbestimmungsrechte der Bürgerinnen und Bürger vor Ort gehen. Global agierende Internetdienste, die ihre Dienstleistungen ausdrücklich an Nutzer innerhalb Deutschlands richten, sind grundsätzlich auf die Einhaltung des nationalen bzw. europäischen Datenschutzrechts verpflichtet. Eine abschließende Klärung der Fragen der Zuständigkeiten und des anzuwendenden Rechts muss die geplante Reform des Datenschutzrechts durch die EU bewirken. Es ist jedoch nicht zu erwarten, dass die neuen europäischen Regelungen vor 2014 in Kraft treten.

Bis auf Weiteres stehen uns daher zunächst nur die Instrumentarien zur Verfügung, die uns der Gesetzgeber zur Sicherung des geltenden Datenschutzstandards der Bürgerinnen und Bürger an die Hand gegeben hat. Dabei sind alle rechtlichen Möglichkeiten auszuschöpfen. Gerade bei der Einführung neuer Risikotechnologien, wie etwa der automatischen Gesichtserkennung im Zusammenhang mit sozialen Netzwerken, ist entscheidend, dass die Nutzer ausreichend über die Datenverwendung informiert werden und sie über die Verwendung und Preisgabe der eigenen Daten selbst entscheiden können. Hier müssen die Standards des geltenden nationalen bzw. europäischen Datenschutzrechts Beachtung finden. Es ist und bleibt eine der vordringlichsten Aufgaben unserer Dienststelle, den Schutz der Grundrechte Betroffener gerade auch in Zeiten des digitalen Wandels und der unklaren Verantwortlichkeiten sicherzustellen.

2. Datenschutz als Aufgabe konsensualer Steuerung

In einer digitalen Welt, deren Treibstoff Informationen mit Personenbezug sind, ist die Datenschutzaufsicht längst nicht mehr auf die eindimensionale Funktion einer rechtlichen Kontrollinstanz beschränkt. Wenn auch die Aufgabe, sich – wie oben bereits dargestellt – schützend vor die digitalen Grundrechte der Bürger zu stellen, gerade angesichts einer globalen Vernetzung und einer entgrenzten Verantwortlichkeit für den Schutz des Einzelnen zu deren Kernbereich gehört, ist der Funktionsumfang dadurch doch noch längst nicht erschöpfend beschrieben.

Die moderne Datenschutzbehörde muss sich der Grenzen der hierarchischen Steuerung und ihrer Reibungsverluste stets bewusst sein. Allein durch den externen Zwang aufsichtsrechtlicher Maßnahmen, seien sie nun präventiver oder repressiver Natur, lässt sich eine nachhaltige Anerkennung und Einsicht in die Regelungsziele des Datenschutzes bei den Adressaten von Rechtsnormen nicht herstellen.

Vor dem Hintergrund einer Rechtsordnung, die durch die Fliehkraft der Dynamik technischer Prozesse auf Fragen nach dem Schutz der Privatsphäre häufig keine passenden Antworten bereithält, sowie einer komplexen Verwendung von Daten zu gänzlich unterschiedlichen ökonomischen, kulturellen und sozialen Zwecken, kann nicht allein auf die zwangsbewehrte Kraft des Rechts vertraut werden. Jenseits eindeutiger Zuschreibungen innerhalb der Kategorien rechtlich zulässiger/ unzulässiger Verhaltensweisen bestehen hier durchaus Handlungskorridore, in denen sich normergänzende Lösungen, gerade auch unter Beteiligung der verantwortlichen Stellen selbst, als hilfreich erweisen können. Konsensorientierte Steuerungsmaßnahmen sowie die Aktivierung der Eigeninitiative und Selbstverantwortungspotentiale Daten verarbeitender Unternehmen führen in der Praxis zu Steigerungen des Datenschutzniveaus. Diese können besonders nachhaltig sein, weil sie häufig dem Eigeninteresse der verantwortlichen Stellen entsprechen und in eine Win-Win-Situation zwischen Betroffenen, Unternehmen sowie letztlich auch der Kontrollbehörde münden.

2.1 Steuerungspotentiale und Grenzen von Verhandlungslösungen

Im Berichtszeitraum hat es eine Reihe von Erfolgen durch Selbstverpflichtungserklärungen bzw. normkonkretisierenden sowie normergänzenden Absprachen mit Daten verarbeitenden Unternehmen gegeben, die allerdings z.T. häufig erst nach langen und kontroversen Verhandlungen mit den jeweiligen Unternehmen erzielt werden konnten.

Hierzu gehört zunächst die Verfahrensgestaltung zum Panorama-Dienst Google Street View. Insbesondere durch die Einräumung eines Vorab-Widerspruchsrechts konnte erreicht werden, dass das Recht auf informationelle Selbstbestimmung deutschlandweit Berücksichtigung fand und von tausenden Bürgern in Anspruch genommen und umgesetzt wurde.[5)]

Ebenfalls nach Verhandlungen konnte erreicht werden, dass Google sich bereit erklärte, beim Einsatz von Google Analytics die Forderungen des Beschlusses des Düsseldorfer Kreises zur Reichweitenmessung aus dem November 2009[6)] umzusetzen. Insbesondere betrifft dies die Zusage, erhobene IP-Adressen in Europa zu anonymisieren.[7)] Nach Umsetzung der Maßnahmen und unter der Einhaltung bestimmter Verfahrensvorgaben[8)] durch die privaten Webseitenbetreiber sehen wir daher nach Abstimmung

[5)] Dazu siehe unter IV.3.4

[6)] Dazu TB 2008/2009, S. 105 f.

[7)] S. unter IV.4.1.

[8)] Näher unter IV.4.1

im Düsseldorfer Kreis von einer Beanstandung des Einsatzes von Google Analytics durch Unternehmen bis auf Weiteres ab.

Eine Überprüfung des stadteigenen Webportals erbrachte, dass auf den Seiten von hamburg.de eine Tracking-Software eingesetzt wurde, die den Anforderungen des Datenschutzrechts und dem Telemediengesetz nicht entsprach. Der Einsatz dieser Software war jedoch in einen größeren Kontext eingebunden und betrifft darüber hinaus alle größeren Online-Medien in Deutschland, für die sie als einheitliches Verfahren zur Reichweitenmessung zur Anwendung kommt. Auch hier gelang es, in intensiven und konstruktiven Gesprächen mit den beteiligten Stellen sowie hamburg.de eine tragfähige Lösung für die Web-Reichweitenmessungen zu erzielen. Das nunmehr angebotene Verfahren reicht weit über die Grenzen Hamburgs hinaus und betrifft den gesamten Bereich der nationalen Online-Medien.[9)]

Letztlich wurde der sog. Friend-Finder, mit dem Facebook sich über die E-Mail Accounts der eigenen Nutzer Kontaktdaten dritter Personen verschafft, um bei diesen für einen Eintritt in das Netzwerk zu werben, auf eine datenschutzrechtlich tragfähige Grundlage gestellt. Künftig sind die Nutzer für das Versenden von Freundschaftsanfragen selbst verantwortlich. Facebook verpflichtete sich zu hinreichenden Informationen von Nicht-Nutzern über den Erhalt von Einladungen und räumte diesen das Recht ein, den Freundschaftsanfragen zu widersprechen.[10)]

Die hier gefundenen Lösungen beruhen nicht unwesentlich auch auf der Einsicht der verantwortlichen Stellen, dass die bisherigen Angebote den datenschutzrechtlichen Normen nicht entsprechen. Dennoch ist ihre Umsetzung letztlich das Ergebnis von zum Teil sehr kontroversen Verhandlungen, bei denen wir zunächst den Einsatz rechtlicher Instrumente zurückgestellt haben.[11)]

In all den angesprochenen Verfahren zeigt sich, dass eine hierarchische Steuerung mangels klarer rechtlicher Vorgaben an ihre Grenzen stößt. Da trotz zwischenzeitlicher Ankündigung durch den damaligen Bundesinnenminister, ein Rote-Linie-Gesetz zum Schutz vor besonders schweren Eingriffen in das Persönlichkeitsrecht zu erlassen, offensichtlich keine konkreten Ansätze zur Reformierung der Regelungsstrukturen auf Bundesebene

[9)] Unter IV.4.2

[10)] Unter IV. 3.2.

[11)] Dabei bleibt darauf hinzuweisen, dass bei den einzelnen Referenzbereichen unterschiedliche Eingriffs- und Gestaltungsmöglichkeiten bestehen: Während Street View und Friend-Finder direkt der behördlichen Kontrolle unterliegen, gibt es beim Einsatz von Tracking-Software keine rechtlichen Verpflichtungen zur Produktverantwortung. Diese trifft vielmehr die einzelnen Webseitenbetreiber.

mehr verfolgt werden, ist von einem jahrelangen Fortbestehen des bisherigen Regelungsdefizits auszugehen.

Das Datenschutzrecht stammt im Wesentlichen noch aus der analogen Zeit und hält damit für die neuen Herausforderungen der digitalen Welt keine angemessenen Antworten bereit. So erweist sich etwa der Personenbezug von Daten als Schlüsselbegriff für die Anwendung des Datenschutzrechts mehr als fragil. Solange nicht zweifelsfrei geklärt ist, ob dynamische IP-Adressen oder das Speichern von Mac-Adressen beim Scannen von WLAN-Netzen dem Datenschutzgesetz unterliegen, fallen eine sachgerechte Auslegung der Normen sowie deren Vollzug schwer. Gleiches gilt für den Personenbezug im Zusammenhang mit der Veröffentlichung von Gebäudeansichten und Grundstücksansichten im Internet. Ebenfalls rechtlich unklar ist das Verhältnis zwischen dem Telemediengesetz und dem Datenschutzgesetz beim Einsatz von Tracking-Software.

Solange Antworten zu grundsätzlichen Rechtsfragen nicht vom Gesetzgeber oder zumindest durch Grundsatzentscheidungen der Judikative vorgezeichnet sind, können Selbstverpflichtungszusagen der datenverarbeitenden Stellen gegenüber den Aufsichtsbehörden durchaus dazu beitragen, den Schutz der Daten Betroffener zu verbessern. In diesem Sinne ist es der Dienststelle in dem vergangenen Berichtszeitraum gelungen, zu nationalen, aber auch internationalen Verbesserungen des Datenschutzniveaus beizutragen.

Erfolgreiche normkonkretisierende Verpflichtungen setzen die Bereitschaft gerade auf Seiten der Daten verarbeitenden Stellen voraus. Letztlich ist die Suche nach Kompromissen aber kein endloser Diskurs, sondern ein Verfahren, in dem es auszuloten gilt, wie die Rechte Betroffener nach Maßgabe der Einsichts- und Freiwilligkeit der verantwortlichen Stellen zu schützen sind. Ziehen sich Verhandlungen – wie beim Einsatz der Gesichtserkennungssoftware durch Facebook – über Monate hinweg ohne greifbare Ergebnisse in die Länge,[12)] bleibt keine andere Wahl, als die verfassungsrechtliche Schutzpflicht gegenüber dem informationellen Selbstbestimmungsrecht der Bürgerinnen und Bürger durch die strikte Anwendung der gesetzlichen Eingriffsinstrumentarien gerade und trotz bestehender rechtlicher Unwägbarkeiten zu erreichen.

Ob der Abschluss eines branchenweiten Verhaltenskodex im Bereich der sozialen Netzwerke künftig zu einer Stärkung des Datenschutzniveaus beitragen kann, wird sich im Verlauf der Gespräche herausstellen, die derzeit im Bundesministerium des Inneren zwischen den beteiligten Akteuren,

[12)] Dazu siehe unter IV. 3.3

insbesondere den Vertretern der wichtigsten sozialen Netzwerke sowie den Datenschutzaufsichtsbehörden, geführt werden. Freiwillige Selbstverpflichtungen oder Verhaltensregeln – und dies gilt ganz allgemein – dürfen jedenfalls die Einhaltung und Umsetzung des geltenden Datenschutzrechts nicht ersetzen, sondern können diese nur fördern. Die Erreichung dieses Zieles erscheint zumindest problematisch, wenn sich hieran Firmen beteiligen, die nicht einmal bereit sind, den gesetzlichen Mindeststandard einzuhalten.

2.2 Datenschutz als Aufgabe betrieblicher und behördlicher Selbstverantwortung

Daten verarbeitende Unternehmen müssen ein starkes Eigeninteresse daran haben, dem Datenschutz einen hohen Stellenwert einzuräumen. Das Datenschutzniveau, das ein Unternehmen seinen Kunden bzw. Nutzern bietet, schafft Vertrauen in seine Produkte und Dienstleistungen und kann dadurch einen signifikanten Wettbewerbs- und Standortvorteil darstellen.

Ein Schlüssel für die organisatorische Aktivierung von Selbststeuerungskompetenzen des Datenschutzes in den Betrieben, aber auch in den ebenfalls kundenorientiert ausgerichteten Behörden ist die Bestellung von internen Datenschutzbeauftragten. Diese haben eine Mittlerfunktion zwischen der datenverarbeitenden Stelle, für die sie tätig werden, und den Kunden bzw. Nutzern, die dem Unternehmen oder der Behörde für unterschiedliche Zwecke ihre Daten zur Verfügung stellen.

Im letzten Tätigkeitsbericht haben wir bereits darauf hingewiesen, dass die Arbeit der Datenschutzbeauftragten vor Ort ein wichtiger Baustein für ein modernes, die betrieblichen und behördlichen Kompetenzen zur Eigensteuerung einbeziehendes Konzept des Datenschutzes ist.[13)] Mit Blick auf die zwischenzeitlich behördlicherseits bestellten Datenschutzbeauftragten ist hier durchaus eine positive Entwicklung innerhalb der FHH zu verzeichnen.[14)]

Im abgelaufenen Berichtszeitraum haben wir damit begonnen, die Bestellungspraxis der betrieblichen Datenschutzbeauftragten von Hamburger Unternehmen in den unterschiedlichen Branchen bei mehr als 700 Unternehmen abzufragen.[15)] Zur Verifizierung der Angaben wurden stichprobenweise Überprüfungen der Antworten der Betriebe durchgeführt.

[13)] Dazu siehe TB 2008/2009, S. 11 ff.

[14)] Ohne behördlichen Datenschutzbeauftragten war nach wie vor die Innenbehörde bzw. die Polizei Hamburg, hier soll jedoch nach Information kurz vor Redaktionsschluss eine Stellenbesetzung erfolgen.

[15)] Unter IV.12.3.

Die Initiative hatte zur Folge, dass die Unternehmen hinsichtlich ihrer Verpflichtung zur Bestellung sensibilisiert wurden. Gleichzeitig konnten wir in vielen Fällen den Petenten erfolgreich raten, ihre Eingaben zunächst den uns bekannten betrieblichen Datenschutzbeauftragten vor Ort vorzulegen, um diesen die Gelegenheit zu geben, den Beschwerden quasi im Rahmen eines dem Beschwerdeverfahren vorgeschalteten Clearing-Verfahrens abzuhelfen. Die Statistik des zurückliegenden Berichtszeitraums belegt, dass dieses „Vorverfahren" durchaus bei den Bürgerinnen und Bürgern, aber auch bei den Beauftragten sowie den verantwortlichen Stellen auf Akzeptanz stößt.[16)]

Im Ergebnis zeigt sich: Eine stärkere Einbeziehung der Datenschutzkompetenz vor Ort dient dem mündigen Bürger zur eigenen Rechtsverfolgung und ermöglicht den Unternehmen bzw. Behörden, individuelle Beschwerden ohne den externen Druck unter Wahrung der Autonomie der Betriebsabläufe selbstverantwortlich beizulegen. Das Instrument der Datenschutzbeauftragten optimiert daher für alle Beteiligten das Beschwerdemanagement und kann dazu beitragen, die Aufsichtsbehörden erheblich zu entlasten.

Wir werden in den nächsten Jahren die positiven Ansätze im Bereich der eigenverantwortlichen Steuerung fortsetzen und uns für eine intensivierte Einbeziehung betrieblicher bzw. behördlicher Selbststeuerungskompetenzen weiter einsetzen.

3. Selbstdatenschutzkompetenz fördern – Datenschutz als Bildungsaufgabe

Für den Schutz der eigenen Daten ist nicht nur die für die Datenverarbeitung verantwortliche Stelle, sondern in erster Linie auch der Einzelne selbst verantwortlich. Bürgerinnen und Bürger müssen daher in der Lage sein, sich eigenverantwortlich in der digitalen Welt zu bewegen. Dies gilt vor allem im Hinblick auf die vielen Gratis-Dienste, die das Internet bietet. Jedem, der die vielfältigen Angebote für eigene Zwecke nutzt, sollte bewusst sein, dass die Eintrittskarte zumeist über die eigenen hierfür eingesetzten Daten gelöst wird.

Ob und in welchem Ausmaß die individuelle Nutzung erfolgen soll, ist eine autonome Entscheidung des mündigen Nutzers. Hier kann und darf die

[16)] Im Verlauf des Jahres 2010 konnten 110 Beschwerden auf unsere Anregung hin durch die Petenten zunächst an die betrieblichen sowie behördlichen Datenschutzbeauftragten zur Klärung weitergegeben werden. Bis auf 8 Fälle, in denen eine Wiederaufnahme der Prüfung durch die Datenschutzbehörden erfolgte, ist es dabei zu einer einvernehmlichen Klärung auf betrieblicher bzw. behördlicher Ebene gekommen. Die Zahlen für 2011 zeigen hier allerdings eine rückläufige Tendenz, was sicherlich auch an der Komplexität der Fallgestaltungen liegt, die häufig einer Verweisung im Interesse einer rechtlichen Abhilfe der Beschwerde von Bürgerinnen und Bürgern entgegen steht.

Aufsichtsbehörde nicht als Treuhänder des Einzelnen tätig werden. Sie kann jedoch dazu beitragen, die Kompetenz des Einzelnen zu fördern, das Datenschutzmanagement in die eigenen Hände zu nehmen.

Dem Ziel, möglichst viele Nutzer aufgeklärt und selbstverantwortlich über die Verwendung und den Einsatz der eigenen Daten entscheiden zu lassen, stehen nicht selten die mitunter bewusst intransparent gefassten Nutzungsbedingungen der Anbieter gegenüber. Hier dokumentieren die Angebote des Web 2.0 erhebliche Defizite. Neben der zu gewährenden Transparenz durch die Stellen selbst steht für uns aber auch die Information und Aufklärung der Nutzer im Vordergrund. Gerade auch Bildungs- bzw. Weiterbildungsangebote sowie ganz allgemein Informationen für Nutzer oder künftige Nutzer stellen ein wichtiges Instrument zur Hebung des allgemeinen Datenschutzniveaus dar.

Der technische Fortschritt und die Kulturtechnologie des Internets sind für sich genommen ambivalent: Sie können sehr viel Positives zur Entfaltung des Einzelnen beitragen. Wer die vielfältigen Angebote nutzen möchte, sollte jedoch auch über die Risiken und Gefahren informiert sein, die bei der Nutzung von Internetdiensten für das informationelle Selbstbestimmungsrecht bestehen. Das gilt in besonderem Maße für Kinder und Jugendliche, die mit den digitalen Medien aufwachsen.

Der Umgang mit unseren Daten bestimmt zunehmend unseren Lebensweg. Datenschutz ist daher in hohem Maße auch Bildungsaufgabe. Zentraler Ort, an dem die Datenschutzkompetenz von Kindern und Jugendlichen vermittelt werden muss, sind die Schulen. Wir haben daher mit der Initiative „Meine Daten kriegt ihr nicht!“ zusammen mit anderen Partnern ein Projekt ins Leben gerufen, das allen Hamburger Schulen helfen soll, das Thema Datenschutz in den Unterricht einzubringen. Anfang 2011 wurde hierzu ein Leitfaden zur Lehrerfortbildung der Öffentlichkeit vorgestellt.[17)] Mit der Informationsbroschüre über ein Konzept zur Vorbereitung einer Unterrichtseinheit Datenschutz liegt ein zentraler Baustein für eine Selbstbefassung der Schulen und der einzelnen Lehrkräfte mit der Thematik vor.

Im Verlauf des letzten Jahres hat sich jedoch auch gezeigt, dass das Ziel eines breiten, alle Schulen hamburgweit erreichenden Unterrichtsangebots mit dem gezielten Ansprechen einzelner Schulen sowie dem Veranstalten von Workshops vor Ort kaum zu erreichen ist. Angesichts mehrerer hundert Hamburger Schulen erschweren sowohl die personelle Ausstattung der Dienstelle, als auch das eher verhaltene Interesse von Schulen an einer freiwilligen Teilnahme an einer Fortbildungsveranstaltung die Errei-

[17)] Dazu siehe unter III.8.1.

chung des Ziels einer nachhaltigen Verankerung der Datenschutzkompetenzförderung im Unterricht.

Natürlich werden wir unser Angebot einer Lehrerfortbildung auch weiterhin für interessierte Schulen anbieten. Die überaus positive Aufnahme unseres Projekts, dort, wo wir es vorstellen konnten, ist uns auch künftig Ansporn. Die Initiative bedarf mittelfristig jedoch weitergehender Impulse, damit die Schulen, an denen eine Lehrerfortbildung stattfindet, nicht einsame Leuchttürme in der Hamburger Schullandschaft bleiben.

Die Fähigkeit zum Selbstdatenschutz darf kein Privileg von wenigen sein. Jedes Kind hat ein Recht darauf zu erlernen, wie man sich in der digitalen Welt sicher bewegt. Die Initiative „Meine Daten kriegt ihr nicht!“ zielt daher darauf ab, dass diese Bildungschance sich für alle einlöst. Gefordert sind neben den Schulen und Lehrkräften gerade auch die für die Organisation von Bildungsprozessen zuständigen Stellen. So wäre etwa die Einführung der Datenschutzkompetenz in die Rahmenlehrpläne ein zentraler Beitrag zur Verankerung der Initiative im hamburgischen Schulalltag.

Wir werden im neuen Berichtszeitraum mit den unterschiedlichen Akteuren Gespräche suchen, um weitere Schritte einzuleiten, damit unsere Initiative einer Datenschutzkompetenzförderung in den Schulen möglichst nachhaltig integriert wird.

4. Zur personellen Situation der Dienststelle

Die personelle Situation der Dienststelle war bereits im letzten Tätigkeitsbericht anlässlich der Eingabenstatistik angesprochen worden.[18)] Sie ist nach wie vor stark angespannt. Vor dem Hintergrund einer rasanten Entwicklung der digitalen Technologien und einer immer stärker um sich greifenden Kommerzialisierung personenbezogener Daten ist die Bedeutung des Datenschutzes in den letzten Jahren erheblich gestiegen. Indikator für das Arbeitspensum der Dienstelle ist die signifikante Zunahme von Eingaben von Bürgerinnen und Bürgern, deren Bearbeitung immer mehr personelle Ressourcen in Anspruch nimmt. Dabei ist bei einer nahezu Verdreifachung der Eingaben in den letzten 10 Jahren die personelle Ausstattung der Dienststelle im entsprechenden Zeitraum weitgehend konstant geblieben.[19)]

Durch diese Situation ist die Dienststelle in einigen Bereichen bereits derzeit auf reaktives Handeln beschränkt. Die erforderlichen Kapazitäten für ein präventives Handeln im Wege der anlassunabhängigen Kontrollen

[18)] TB 2008/2009, S. 2f.

[19)] TB, TB 2008/2009, S. 3.

öffentlicher und nicht-öffentlicher Stellen sind nicht vorhanden. Wichtige Vorhaben wie die Überprüfung der von öffentlichen Stellen betriebenen Videoanlagen, die im letzten Jahr mit einer umfassenden Ermittlung aller Anlagen bei den Behörden begonnen wurde[20], oder auch die Durchführung nachbereitender Überprüfungen von umgesetzten IT- Projekten im öffentlichen Bereich entwickeln sich daher eher schleppend oder waren im Verlauf des letzten Jahres nicht durchführbar. Gleiches gilt für präventive Kontrollen im nicht-öffentlichen Bereich, die nur in einem geringen Umfang möglich waren. Hier stehen wir mit fünf Mitarbeitern nicht nur den 160.000 zu kontrollierenden Unternehmen in Hamburg gegenüber, vielmehr haben mit Google und Facebook auch noch zwei global agierende Internet-Konzerne ihre nationalen Hauptniederlassungen in Hamburg. Daraus folgt nicht nur, dass wir deutschlandweit Ansprechpartner für Bürgerinnen und Bürger bei Beschwerden gegen diese Unternehmen sind, sondern auch, dass unsere Dienststelle immer stärker in den Fokus der überregionalen und internationalen Presse geraten ist. Die Beantwortung von durchschnittlich ca. 30 Presseanfragen pro Monat (nach statistischer Erhebung von März bis Dezember 2011) bindet personelle Kapazitäten, die dem operativen Bereich entzogen werden.

Maßnahmen zur Verbesserung der personellen Situation wurden durch uns bereits in der Vergangenheit eingeleitet: So haben wir uns in den letzten Jahren um personelle Verstärkung aus Projekten über das Personalamt (Wiedereingliederung, Integration von Rückkehrern) bemüht und von dort auch erhalten. Neben den 14,6 regulären Stellen im Bereich des Datenschutzes unterstützen uns auf diesem Weg vier Personen mit 3,1 Stellenanteilen. Eine weitere Stelle wurde uns durch das Personalamt für Anfang 2012 angeboten. Die externe Finanzierung von zwei dieser Stellen lief bzw. läuft ab 2012 ganz oder teilweise aus. Um die Mitarbeiter, die unsere Arbeit wesentlich unterstützen und auch selbst an einer Weiterbeschäftigung im Bereich des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit interessiert sind, künftig bei uns zu halten, müssen die Stellen zumindest anteilig aus eigenen Mitteln gegenfinanziert werden. Dies kann aber auf Dauer mit den beschränkten eigenen Haushaltsmitteln nur eine Brückenlösung sein. Die Absicherung der bestehenden Personaldecke ist daher eine Minimalforderung, die faktisch keine Verstärkung für die Dienststelle bedeutet, aber immerhin die bisherige Qualität und Quantität der Aufgabenerfüllung sichert.

Ohne diese zusätzlichen Kapazitäten, die in den organisatorischen Ablauf der Dienststelle fest eingeplant sind, wäre die Abarbeitung der stetig zu-

[20] Hierzu siehe unter I.1.2.

nehmenden Aufgaben im Bereich des Datenschutzes nicht mehr zu gewährleisten. Auf Dauer ist es daher zur Aufrechterhaltung eines effizienten Dienstbetriebs nötig, die vier derzeit auf Basis befristeter Abordnungen beschäftigten Mitarbeiter durch neue, eigene Stellenanteile dauerhaft abzusichern.

Für eine Weiterbeschäftigung dieser Mitarbeiter müssten im Hinblick auf den Gesamthaushalt zunächst keine neuen Haushaltsmittel aufgebracht werden, da die betroffenen Mitarbeiter bereits bei der FHH beschäftigt sind. Wir werden unsere Forderung nach einer Konsolidierung der personellen Ressourcen in den kommenden Monaten noch einmal mit einer umfassenden vergleichenden Analyse unserer Dienststelle untermauern.

II. INFORMATIONS- UND KOMMUNIKATIONSTECHNIK

1. Migration Datennetz und Anwendungen der Polizei zu Dataport

Seit mehreren Jahren erfüllt die Polizei Hamburg Ihre datenschutzrechtlichen Dokumentationspflichten nur unvollständig. Das neu entwickelte Verfahrenskataster muss jetzt unverzüglich genutzt werden, um diesen Mangel zu beheben.

In den beiden letzten Tätigkeitsberichten (vgl. 21.TB, II 2.7 und 22.TB, II 2.7) berichteten wir von der Übergabe des Polizei-Netzwerks an Dataport und insbesondere von den Mängeln in der Dokumentation. Die Polizei Hamburg übergab ihr vorher selbst betriebenes Netzwerk für die eingesetzte PC-Hardware an den IT-Dienstleister Dataport (offizieller Übergabetermin 01.10.2007). Zahlreiche Informations-, Auskunfts- und Vorgangsbearbeitungsverfahren der Polizei sind in die Betreuung von Dataport übergegangen. Es bestanden erhebliche Bedenken, ob die realisierten Datenschutz- und Datensicherheitsstandards des Dienstleisters ausreichen, um den notwendigen Schutzbedarf für das Polizeinetz zu gewährleisten.

Diese Bedenken sollten durch die Polizei Hamburg und den HmbBfDI nachträglich gemeinsam bewertet werden, um daraus eventuelle Handlungsnotwendigkeiten abzuleiten und auch die Vollständigkeit der erforderlichen datenschutzrechtlichen Unterlagen festzustellen.

Das in 2010 abgesprochene Vorhaben, die beim HmbBfDI vorliegenden Dokumente zu vervollständigen, kam nur schleppend voran; das Ergebnis war und ist nicht befriedigend:

- Die Idee einer strukturierten, intelligent vernetzten und alltagstauglichen Strategie zur Erzeugung der datenschutzrechtlich erforderlichen Informationen wurde nicht umgesetzt.
- Externe Hilfe zur Betrachtung der BSI-Grundschutzkonformität hielt die Polizei Hamburg nicht für notwendig.
- Auftaktveranstaltungen zur Darstellung komplexer Verfahren der Polizei Hamburg sind ohne in Aussicht gestellte Folgeveranstaltungen geblieben.
- Der Abschlussbericht eines im letzten Jahr durchgeführten Audits bei der Polizei Hamburg liegt uns trotz mehrfacher Zusage und Nachfrage bis heute nicht vor.
- Eine Projektgruppe Migration Datennetz, die eingerichtet wurde, „um offene Fragen umgehend einer Lösung zuzuführen“, traf sich das erste

Mal im Januar 2011 und das letzte Mal im Februar 2011. Abschließende Lösungen wurden nicht erreicht.

Eine Chance, die festgestellten Mängel der Dokumentationen zu beheben, bietet das Verfahrenskataster. Es entstand unter anderem aus der Reorganisationsnotwendigkeit im IT-Bereich der Polizei Hamburg, ist aber auch geeignet, datenschutzrechtlichen Dokumentationsverpflichtungen Rechnung zu tragen. Wir begrüßen daher das Engagement der damit befassten Mitarbeiter bei der Polizei Hamburg. Gerne haben wir unseren Beitrag dazu geleistet. Gleichzeitig hoffen wir, dass dieses Projekt die notwendige Priorität erhält, um nicht nur die Polizei Hamburg selbst voranzubringen, sondern auch als Informationsbasis für eine gute zukünftige Zusammenarbeit zu dienen.

Die Berufung eines behördlichen Datenschutzbeauftragten bei der Polizei Hamburg könnte zu einer Verbesserung in der Bearbeitung datenschutzrechtlicher Fragestellungen führen. Mit einem festen Ansprechpartner vor Ort würde auch die Zusammenarbeit für uns mit einer solch großen Organisation wie der Polizei Hamburg erleichtert.

2. Neuer Zugang aus dem Internet zu IT-Verfahren im FHH-Netz

Der Zugang sollte regelmäßig auf Sicherheitslücken überprüft werden.

Mit dem IT-Verfahren Zuvex (Zugang von extern) wird eine Infrastrukturkomponente bereitgestellt, mit der ein Zugriff auf IT-Verfahren im FHH-Netz von außerhalb ermöglicht wird. Dieses Verfahren ist seit Ende November 2011 zunächst für die Mitarbeiterinnen und Mitarbeiter der FHH und ab Mitte 2012 auf Antrag auch für bekannte externe Kunden wie z. B. Berater konzipiert, denen mit diesem Verfahren ein Zugriff über das Internet ermöglicht wird. Zu einem späteren Zeitpunkt soll das Verfahren auch für anonyme externe Nutzer mit eingeschränkten Möglichkeiten zur Verfügung gestellt werden.

Für die technische Realisierung wird auf die Software „Forefront Unified Access Gateway (UAG)“ von Microsoft zurückgegriffen. Das UAG soll als Sicherheitsgateway den Zugriff auf ausgewählte Anwendungen im FHH-NET über das Internet ermöglichen. Als erste Anwendung wird hierbei der Zugriff auf das behördenübergreifende Inforamationsportal im Intranet der FHH, das FHHportal, zur Nutzung freigegeben. Beim UAG werden Anwendungen nicht direkt im Internet veröffentlicht, sondern es wird ein kontrollierter Weg für den Zugriff auf die Anwendung aus dem Internet heraus zur Verfügung gestellt. Das UAG stellt dabei einen Proxy dar, der als vermeintliches Zielsystem in Erscheinung tritt und so die wahre Adresse des Zielsystems vor dem Nutzer verbirgt. Auf Applikationsebene wird eine

Filterung der Daten vorgenommen, und das UAG kann so konfiguriert werden, dass in Abhängigkeit der zugreifenden Clients der Zugriff erlaubt, eingeschränkt erlaubt oder verweigert wird. Der Zugriff wird nur erlaubt, wenn die vom UAG angestoßene Endgerätekontrolle ergeben hat, dass auf dem Endgerät eine Firewall aktiviert ist und ein aktuelles Virenschutzprogramm läuft. Schlägt diese Endgerätekontrolle fehl oder zeigt nicht das für die Anwendung erforderliche Ergebnis, wird der Zugriff verweigert oder eingeschränkt. Es wird vom UAG außerdem festgestellt, ob es sich um einen Client des FHHNET handelt (managed client, z. B. das Gerät eines Telearbeiters) oder um einen unbekannten Client (unmanaged). Bei einem unbekannten Client wird der Download von Dokumenten unterbunden.

Für die Endgerätekontrolle ist auf dem Client eine Active-X-Komponente bzw. ein Java-Plugin zu installieren. Auf Clients des FHHNET wird dies durch eine zentrale Verteilung installiert, die Komponente wird durch das ITAB freigegeben. Auf privaten PCs muss die Komponente mit Administrationsrechten vom Nutzer installiert werden. Ohne diese Komponente ist eine Endgerätekontrolle nicht möglich.

Für das IT-Verfahren Zuvex wurde von der Finanzbehörde eine Risikoanalyse vorgelegt und uns zur Stellungnahme zugeleitet. Dabei haben wir kritisiert, dass gerade die mit dem Verfahren neu hinzugekommenen Risiken für die Nutzer nicht ausreichend behandelt werden:

- Da mit dem Verfahren Zuvex eine definierte Öffnung in den Schutz des FHH-Netzes zugelassen wird, sollte sichergestellt werden, dass damit keine Möglichkeiten einhergehen, die von Externen zu einem unberechtigten Zugriff ausgenutzt werden können. Dies darf weder durch die Nutzung der eingesetzten Komponenten noch durch die vorgenommenen Einstellungen erfolgen, die sehr komplex und daher anfällig für Fehlkonfigurationen sind. Aus diesem Grund sollten durch regelmäßige Penetrationstests mögliche Sicherheitslücken aufgedeckt und anschließend unverzüglich behoben werden. Solche Tests sind auch bei anderen definierten Zugängen über das Internet etwa beim Hamburg-Gateway Bestandteil der Sicherheitsmaßnahmen.
- Zur Endgerätekontrolle muss der Nutzer eine technische Komponente auf seinem Rechner installieren, ohne dass transparent wird, welche Funktionen diese genau ausführt und ohne dass z. B. durch ein Zertifikat sichergestellt ist, dass darüber hinaus keine weiteren Aktivitäten auf dem Client erfolgen.
- Dem Nutzer wird nicht angezeigt, welche Dateien und Verzeichnisse standardmäßig zur Nutzung von Zuvex angelegt werden.

- Es sollte sichergestellt werden, dass im Zuge einer Deinstallation die angelegten Verzeichnisse und Dateien rückstandslos automatisch gelöscht werden.

3. Internet-Protokoll Version 6 (IPv6)

Die Umstellung auf eine neue Technik im Internet ist im Gange. Deren datenschutzgerechte Gestaltung muss frühzeitig berücksichtigt werden.

Dem Internet steht eine Revolution ins Haus. Zugegeben, es handelt sich eher um eine leise Revolution. Denn gemeint sind hier nicht Schlagwörter wie „Web 2.0“ oder „Cloud Computing“, sondern ein Umbau gewissermaßen im Maschinenraum des Internet. Das bisherige, seit Anbeginn des Internet benutzte „Internet Protocol“ wird von seiner aktuellen Version 4 (IPv4) auf die künftige Version 6 (IPv6) umgestellt (eine Version 5 hat es übrigens nie gegeben).

So undramatisch dies klingen mag, bringt IPv6 eine Reihe von datenschutzrelevanten Veränderungen mit sich, die über kurz oder lang jeden Internet-Nutzer betreffen, egal ob er seinen DSL-Anschluss, sein Smartphone, einen öffentlichen Hotspot oder das Gerät an seinem Arbeitsplatz benutzt. Denn IPv6 hat bereits in mehr Geräten Einzug erhalten, als den meisten Anwendern bewusst ist. Aktuelle Betriebssystemversionen können bereits mit beiden Versionen umgehen, ohne dass dies an die Oberfläche der Fenster, Browser oder Apps dringt.

Die datenschutzgerechte Gestaltung dieser Technik stellt daher eine wichtige Aufgabe dar, der wir uns frühzeitig angenommen haben. Durch Öffentlichkeitsarbeit, Mitwirkung an einer Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie Beteiligung an einer Arbeitsgruppe auf Länderebene haben wir dazu beigetragen, dass die Datenschutzfragen bei IPv6 in den Fokus genommen wurden und mittlerweile auf breiter Basis öffentlich diskutiert werden. Sowohl Anforderungen als auch Lösungsvorschläge für die verschiedenen Datenschutzaspekte wurden formuliert und werden weiter verfeinert. Dabei spielt die Mitwirkung der Wirtschaft (Access- und Content-Provider, Hersteller von Hard- und Software) eine besondere Rolle. Aber auch der einzelne Nutzer ist gefragt, nicht zuletzt in seinem Konsumverhalten.

Worum geht es im Einzelnen?

Das gravierendste Merkmal von IPv6 ist die geradezu explosionsartige Vergrößerung des Adressraums. Während bei IPv4 ca. 4 Milliarden verschiedene Adressen zur Verfügung stehen, können mittels IPv6 ca. 340 Sextillionen Geräte adressiert werden. Dies reicht theoretisch aus, um jeden Quadratmillimeter der Erde mit mehreren hundert Billiarden

IP-Adressen zu versorgen, d.h. mit mehr Adressen als unter IPv4 für den gesamten Planeten zur Verfügung stehen.

Diese schier unerschöpfliche Menge macht neue Adressierungsmodelle möglich. Während es bei IPv4 aufgrund der Knappheit der Adressen (mittlerweile sind nahezu alle Adressbereiche verteilt) in den meisten Fällen unvermeidlich ist, einem Internetnutzer eine bestimmte Adresse nur solange zur Verfügung zu stellen, wie dieser sie benötigt, um sie anschließend einem anderen Nutzer zuzuweisen (sog. dynamische Vergabe), ist eine solche Bewirtschaftung bei IPv6 nicht mehr erforderlich. Eine feste und dauerhafte Zuordnung einer IPv6-Adresse zu einem bestimmten Nutzer oder Gerät ist möglich (statische Vergabe), ohne an die Grenzen des Adressraums zu stoßen.

Allerdings ist dies aus Datenschutzsicht höchst problematisch. Da die Internetadresse aus technischen Gründen zwingend jedem Internetangebot mitgeteilt wird, könnten die Aktivitäten eines Nutzers allein anhand seiner Adresse webseitenübergreifend zu individuellen Profilen zusammen geführt werden. Wäre die Identität des Inhabers einer Adresse einmal aufgedeckt, könnten alle Anbieter Zugriffe dieser Adresse dem Nutzer direkt zuordnen.

Die Konferenz der Datenschutzbeauftragten hat daher gefordert:

- Internetzugangsanbieter (Access Provider) sollten Kundinnen und Kunden statische und dynamische Adressen ohne Aufpreis zuweisen. Auf Kundenwunsch sollten statische Adressen gewechselt werden können.
- Kundinnen und Kunden sollten mit nutzerfreundlichen Bedienelementen bei der Auswahl der Adressen für jeden von ihnen genutzten Dienst unterstützt werden.

Mit der dynamischen Adressvergabe ist jedoch nur eine Möglichkeit der Nutzeridentifizierung berücksichtigt. Denn sie bezieht sich lediglich auf die eine Hälfte der IPv6-Adresse, den sog. Präfix. Ein weiteres Risiko stellt die andere Hälfte, der Interface Identifier, dar. Dieser ist in der Lage, unabhängig vom Präfix, ein Gerät weltweit eindeutig zu bezeichnen. Dies entspricht auch der Standardmethode, bei der der Interface Identifier aus einem dem Gerät fest zugeordneten, hardwarebasierten Merkmal gebildet wird.

Alternativ sehen die Normen jedoch auch vor, dass hierfür eine Zufallszahl verwendet wird, die nach einer gewissen Zeit neu erzeugt wird. Dieses Verfahren wurde speziell im Hinblick auf den Datenschutz konzipiert und trägt daher die Bezeichnung „Privacy Extensions“. Ob ein Gerät diese Methode

beherrscht und ob sie standardmäßig aktiviert ist, entscheidet der Hersteller des verwendeten Betriebssystems.

Die Forderung der Konferenz der Datenschutzbeauftragten lautet daher:

- Hard- und Softwarehersteller sollten die „Privacy Extensions“ unterstützen und standardmäßig einschalten (privacy by default), um die Wiedererkennung von Nutzenden anhand von Hardwareadressen zu erschweren.

Aufgrund des vollkommen anderen Aufbaus von IPv6- gegenüber IPv4-Adressen ist die Frage der Anonymisierung von IP-Adressen neu zu beantworten. Die für IP-Adressen bestehenden gesetzlichen Nutzungs- und Speicherungsbegrenzungen sind technikneutral und gelten daher auch bei Umstellung auf IPv6. Vor einer weiteren Nutzung der Adressen, z. B. um den ungefähren Standort des Nutzers zu ermitteln (Geolokalisierung), müssen sie daher anonymisiert werden. Hierfür gilt:

- Anbieter von Internetdiensten (Content Provider) dürfen zur Reichweitenmessung nur die ersten 4 Bytes der IPv6-Adresse heranziehen und müssen den Rest der Adresse löschen, denn eine Analyse von Nutzungsdaten ist nach Ansicht der Datenschutzaufsichtsbehörden nur auf der Grundlage anonymisierter IP-Adressen zulässig. Die ersten 4 Bytes sind für eine Geolokalisierung ausreichend.

Die Standards rund um die neue Version IPv6 sehen eine Reihe von expliziten wie impliziten Sicherheitsaspekten vor. Diese reichen von der Verschlüsselung und Authentisierung durch IPSec über neuartige Firewallanforderungen bis zu Fragen der geringeren Sichtbarkeit von Rechnern für eventuelle Angreifer im Rahmen sogenannter Portscans. Soweit anwendbar, sollten Netzwerke und Applikationen alle Sicherheitsfunktionen von IPSec in vollem Umfang nutzen, um die Sicherheit, Integrität und Vertraulichkeit zu gewährleisten.

Allerdings ist in Anbetracht der höheren Komplexität von IPv6 gegenüber IPv4 auch davon auszugehen, dass IPv6-fähige Produkte vielfach noch nicht vollständig ausgereift sind.

Daher gilt:

- Vom Einsatz von IPv6 innerhalb von lokalen Netzen ist aktuell noch abzuraten, wenn dort sensible personenbezogene Daten verarbeitet werden sollen und funktionsfähige Filtereinrichtungen weder zentral noch auf den einzelnen Rechnern im LAN vorhanden und aktiviert sind.

Der gesamte Wortlaut der Entschließung ist unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/82DSK_IPv6.pdf?__blob = publicationFile abrufbar.

4. RMS in der hamburgischen Verwaltung

Die sog. Erweiterte Sicherheit zur Verschlüsselung von E-Mails wurde abgeschaltet. Die als Ersatz hierfür geplante Technik RMS kommt nur mit erheblichen Verzögerungen voran.

Bereits Ende 2009 wurden wir durch die Finanzbehörde über die geplante Einführung eines Rights Management Systems (RMS) im FHHInfonet informiert. Diese Technik soll die sog. Erweiterte Sicherheit ablösen, die im E-Mail-Verkehr der FHH für eine Verschlüsselung der Mails sorgt. RMS bietet die Möglichkeit, sowohl E-Mails als auch Office-Dokumente mit verschiedenen Schutzmechanismen zu versehen und dadurch z. B. zu steuern, wer den Inhalt lesen, kopieren oder drucken darf. Technisch wird dies durch eine Verschlüsselung der Inhalte realisiert.

Hintergrund dieser Umstellung ist der erforderliche Wechsel der Software auf den Mail-Servern von Exchange 2000 zu Exchange 2010, da der Hersteller für die bisherige Version keinen Support mehr anbot. Die für die Erweiterte Sicherheit erforderlichen Techniken (Key Management Server) stehen unter Exchange 2010 nicht mehr zur Verfügung.

Bereits in der Planungsphase des Projekts war klar, dass es keinen nahtlosen Übergang von der Erweiterten Sicherheit zu RMS geben wird, da der erforderliche Fahrplan für die Exchange-Umstellung ein Zeitfenster von mindestens sechs Monaten öffnen würde, währenddessen weder die alte noch die neue Technik zur Verfügung steht. Wir haben kritisiert, dass die Planungen für RMS nicht früher begonnen wurden, konnten die zwingenden Gründe für das Update auf Exchange 2010 jedoch nicht ignorieren. Wir haben uns daher auf folgendes geplante Verfahren eingelassen:

- Die Erweiterte Sicherheit wird zu einem rechtzeitig angekündigten Termin deaktiviert. Die Nutzer erhalten genügend Zeit und technische Unterstützung bei der Sicherung vorhandener verschlüsselter Mails, da auf diese nach der Deaktivierung nicht mehr zugegriffen werden kann.
- RMS wird zum 1.6.2010 für ca. 5000 Nutzer produktiv gesetzt.
- Die Transportverschlüsselung zwischen Outlook als E-Mail-Client und den Exchange-Servern wird aktiviert. Dies stellt eine verschlüsselte Übermittlung, jedoch keine verschlüsselte Ablage der Mails sicher, die zur Wahrung der Vertraulichkeit gegenüber Kollegen oder Administratoren erforderlich ist.

Am 21.4.2010 wurde die Erweiterte Sicherheit in der FHH deaktiviert. Vorab wurden die Nutzer über Möglichkeiten informiert, wie vermieden werden kann, dass Inhalte von Mails danach nicht mehr zugänglich sind.

Wir haben uns zudem bereit erklärt, an einer Pilotierung des RMS teilzunehmen, damit wir uns vorab über die Möglichkeiten und Grenzen der Technik ein eigenes Bild machen können. Im Rahmen dieses Pilotbetriebs kam es immer wieder zu Verzögerungen. Ein wesentlicher Faktor hierfür stellte ein erforderliches Plugin für Outlook dar, für dessen Erstellung eine Drittfirma beauftragt wurde. Hier kam es zu erheblichen Verzögerungen und Mängeln, die dazu führten, dass die Produktivsetzung mehrfach verschoben werden musste. Eine Nutzung ist nunmehr seit September 2011 möglich und erfordert eine gesonderte Beauftragung bei Dataport. Dies sollte mindestens für alle Nutzer geschehen, die per E-Mail mit sensiblen personenbezogenen Daten in der FHH umgehen.

Letztlich kann das Potenzial von RMS jedoch nur dann ausgeschöpft werden, wenn es flächendeckend zur Verfügung gestellt wird. Jeder Teilnehmer könnte dann davon ausgehen, dass alle Empfänger über die Möglichkeit verfügen, mit entsprechend verschlüsselten E-Mails und Dokumenten umzugehen.

5. Notfalldaten auf der elektronischen Gesundheitskarte ohne PIN?

Es ist datenschutzrechtlich sehr kritisch, dass im Zuge der Neuausrichtung der elektronischen Gesundheitskarte auf eine obligatorische Nutzung der PIN beim Schreiben der Notfalldaten verzichtet werden soll.

Die Bundesregierung hat 2009 eine Bestandsaufnahme zur elektronischen Gesundheitskarte (eGK) durchgeführt. Auf dieser Grundlage wurden eine Neuorientierung der eGK beschlossen und die Verantwortlichkeiten neu festgelegt: Die Leistungserbringer (Ärzte und Zahnärzte) werden die alleinige Verantwortung für die medizinischen Anwendungen übernehmen und sich zunächst um den Notfalldatensatz kümmern, der freiwillig auf der eGK gespeichert werden kann. Die Kostenträger (Krankenkassen) sind verantwortlich für das Versichertenstammdatenmanagement und die kassenärztliche Bundesvereinigung (KBV) wird die „adressierte Kommunikation“, den sog. elektronischen Arztbrief, entwickeln.

Mit dem neuen Notfalldatenmanagement soll der bisher geplante Umfang der Daten für diese Anwendung ausgeweitet werden. Zu den in diesem Bereich verarbeiteten Daten sollen künftig gehören:

- Erklärungen, wo Patientenverfügungen und Organspendeerklärung zu finden sind.
- Stammdaten (Name, Anschrift, Notfall-Tel.-Nr., ..).
- Diagnosen (Kodiert).

- Medikation (Arzneimittel, Menge, Wirkstoff).
- Allergien.
- Besondere Hinweise: Schwangerschaft, Kommunikationsstörungen, Weglaufgefährdung.
- behandelnde Ärzte.

Eine sehr wesentliche technische Maßnahme zum Schutz der Daten auf der eGK ist die Nutzung einer PIN. Aufgrund der aufgetretenen Probleme im Anwendungstest wurden von der Gematik technische Veränderungen bei der PIN-Nutzung vorgenommen, insbesondere wurde die enge zeitliche Bindung der erforderlichen PIN-Eingaben stark verändert. Die so geänderten Karten wurden jedoch nicht mehr im Rahmen der Anwendungstests getestet.

Wegen der in den ersten Tests aufgetretenen Mängel bei der PIN-Nutzung sieht das jetzt vorgelegte Konzept des Notfalldatenmanagements vor, dass für das Anlegen von Notfalldaten und die Nutzung der Notfalldaten die PIN-Nutzung nicht initialisiert werden muss. Das erstmalige Anlegen der Notfalldaten erfordert damit nicht mehr wie bisher die vorherige PIN-Eingabe durch den Patienten, mit der die Zustimmung auch technisch abgefragt wird. Der Arzt kann technisch die Notfalldaten auch ohne Zustimmung des Patienten anlegen. Auch jeder weitere schreibende Zugriff durch einen Arzt erfordert keine PIN-Eingabe durch den Patienten.

Technisch soll mit dem neuen Konzept damit erstmalig die Möglichkeit geschaffen werden, schreibend ohne vorherige PIN-Eingabe auf die eGK zuzugreifen. Diese Möglichkeit wurde vorher technisch ausgeschlossen. Eine Beschränkung auf die Notfalldaten ist zwar möglich, aber technisch nicht erzwungen. Somit könnte der Verzicht der PIN-Eingabe auch für weitere Anwendungsfelder genutzt werden.

Auch wenn ein Patient die PIN-Nutzung initialisiert hat, wird die PIN-Eingabe beim Schreiben nicht technisch erzwungen. Somit besteht auch dann für Personen, denen sehr am Schutz ihrer Daten gelegen ist, keine Möglichkeit, ein unbemerktes Anlegen, Schreiben und Löschen der Notfalldaten zu verhindern. Auch für diesen Personenkreis bleibt nur der Schutz durch die organisatorischen Maßnahmen (schriftliche Einwilligung).

Die Ärztekammer betont zwar, dass der Verzicht auf die PIN-Eingabe beim Anlegen und Schreiben eine „Ausnahmesituation“ sei. Dabei ist jedoch zu beachten, dass weder das erstmalige Anlegen noch die laufende schreibende Veränderung in einer Notfallsituation stattfindet. Vor dem Hintergrund der gemachten Äußerungen und der Begründung, dass die Notfall-

daten insbesondere von nicht Technik-affinen Personen, älteren und chronisch Kranken genutzt werde, muss diese Einschränkung jedoch angezweifelt werden, da diese Begründung auch für weitere Anwendungsfälle gilt.

Wir haben uns dafür eingesetzt, dass auf die Eingabe der PIN vor dem erstmaligen Anlegen und beim schreibenden Zugriff nicht verzichtet, sondern stattdessen mit alternativen Maßnahmen die Benutzerfreundlichkeit verbessert wird.

Auch wenn unsere Bedenken nicht aufgegriffen wurden, werden wir weiter die Einführung der eGK kritisch begleiten. Dabei werden wir uns auch weiterhin dafür einsetzen, dass im Rahmen der vorgeschriebenen Testphasen auch die Möglichkeiten zur Wahrnehmung der Betroffenenrechte betrachtet und die datenschutzrechtlichen Anforderungen nicht zurückgestellt werden.

6. Gesetzentwurf zum Hamburger Informationsmanagement (HIM)

Nach vielen Treffen mit der Finanzbehörde auf Arbeitsebene haben wir unsere datenschutzrechtlichen Vorbehalte gegen eine Volltextsuche beim Hamburger Informationsmanagement (HIM) mit Blick auf die notwendige Schaffung einer Rechtsgrundlage, die die Einzelheiten regelt, zunächst zurückgestellt.

Papierlose Verwaltung, eAkte und Dokumentenmanagement sind die Top-Themen in den Organisationabteilungen der Bundes- und Landesverwaltungen. Das entsprechende Projekt der Hamburger Verwaltung ist das „Hamburger Informationsmanagement (HIM)“. Es zielt auf eine durchgehend elektronische Behördenarbeit, egal ob bei einem Vermerk, einer Verfügung oder der gesamten Akte. Ein wesentliches Element von HIM ist eine übergreifende Volltextrecherche in allen zur Verfügung stehenden digitalen Quellen. Davon können auch personenbezogene Daten betroffen sein.

Vereinfacht dargestellt gleicht diese Volltextsuche einer Stichwortsuche bei Google. Der Sachbearbeiter kann nach jedem beliebigen Wort suchen und bekommt eine Trefferliste für die Dokumente seines Aufgabengebiets angezeigt. Das können beispielsweise Begriffe wie „HIV“ oder „Missbrauch“ sein, aber auch Namen von Bürgerinnen und Bürgern oder Kolleginnen und Kollegen. Beliebige personenbezogene Recherchen werden möglich, die nur durch das Aufgabengebiet und die Zugriffsrechte des Sachbearbeiters beschränkt werden. Angesichts der regelmäßigen Fluktuation von Verwaltungsmitarbeitern und der Umorganisation von Aufga-

ben, aber auch einer behördenweiten Rechteverwaltung, sind Fehler und Missbräuche hier kaum auszuschließen.

Die durch HIM möglichen Eingriffe in das informationelle Selbstbestimmungsrecht des Einzelnen machen eine konkrete Rechtsgrundlage für den Einsatz von automatisierten Dokumentationsmanagementsystemen erforderlich. Um dieser Forderung Nachdruck zu verleihen, haben wir nun einen Gesetzentwurf zur „Sicherung des Datenschutzes beim automatisierten Informationsmanagement in der öffentlichen Verwaltung“ vorgeschlagen. Dieser Gesetzesentwurf soll die Grundlage für einen datenschutzgerechten Umgang mit personenbezogenen Daten in HIM schaffen. Darüber hinaus soll er aber auch eine öffentliche Debatte anstoßen, die bei den derzeitigen Bestrebungen zur papierlosen Verwaltung und dem sogenannten „eGovernment-Gesetz“ bislang zu kurz gekommen ist. Mit einer Pressemitteilung haben wir das Projekt im November 2011 auch den Medien vorgestellt.

Regelungsbedarf besteht dabei nicht nur für die einfachen Mitarbeiter, sondern auch für die Zugriffsrechte der höheren Hierarchieebenen. Denn je höher die Stellung, desto umfangreicher kann – entsprechend der hierarchischen Pyramide – der Datenbestand sein, auf den zugegriffen werden kann. Beispielsweise wäre denkbar, dass sich ein Bezirksamtsleiter auf Knopfdruck alle Anliegen eines bestimmten Bürgers anzeigen lässt. Die zentrale Datenhaltung in den Ämtern ermöglicht die Erstellung von Profilen der Bürgerinnen und Bürger in einer Weise, die bislang innerhalb papierener Aktenbestände nicht möglich war.

Es geht uns nicht darum, die digitalen technischen Innovationen, die zu Effizienzsteigerungen der Verwaltung beitragen, zu verhindern, sondern für ihren Einsatz rechtsstaatliche Vorgaben zu machen. Rein verwaltungsinterne Regelungen des Umgangs mit digitalen Informationsmanagementsystemen der Behörden greifen angesichts der hohen Risiken für das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger zu kurz. Vielmehr bedarf es klarer Rechtsnormen, die die Verwaltung an bestimmte gesetzliche Vorgaben und Verantwortlichkeiten binden.

Der Gesetzesvorschlag enthält Bestimmungen über

– die datenschutzrechtliche Verantwortung der Behörden,
– Ausnahmen von der elektronischen Verarbeitung besonders sensibler personenbezogener Daten,
– Normen für Such- und Auswertungsfunktionen, insbesondere die Volltextrecherche,

– ein konsistentes Zugriffskonzept,
– die Übermittlung aus elektronischen Akten und
– die Protokollierung von Zugriffen.

In ersten Gesprächen mit der Finanz- und Justizbehörde sowie dem Staatsarchiv wurde der Gesetzentwurf mit Interesse zur Kenntnis genommen. Wir sind uns bewusst, dass für eine Umsetzung unserer Vorschläge statt eines eigenen Gesetzes auch Änderungen bestehender Gesetze wie z. B. des Hamburgischen Datenschutzgesetzes oder Erweiterungen geplanter eGovernment-Gesetze in Betracht kommen.

7. Mangelnde Sicherheitsvorgaben bei IT-Verfahren mit hohem Schutzbedarf

Die bei Dataport beauftragten und im Rechenzentrum realisierten technischen und organisatorischen Schutzmaßnahmen müssen sich an dem festgestellten Schutzbedarf ausrichten.

Im Hamburgischen Datenschutzgesetz ist unter § 8 Abs. 4 festgelegt, dass vor der Entscheidung über die Einführung oder die wesentliche Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden sollen, die Daten verarbeitenden Stellen zu untersuchen haben, ob und in welchem Umfang mit der Nutzung dieses Verfahrens Gefahren für die Rechte der Betroffenen verbunden sind. Es ist mittlerweile eine gängige Vorgehensweise, dass bei diesen Risikoanalysen der Schutzbedarf der Daten anhand der drei Kategorien „normaler Schutzbedarf“, „hoher Schutzbedarf“ oder „sehr hoher Schutzbedarf“ bewertet wird. Aus dem Schutzbedarf und den Risiken sind die erforderlichen technischen und organisatorischen Schutzmaßnahmen abzuleiten. Diese müssen sich sowohl auf die neue Anwendung als auch auf die Infrastruktur der genutzten Rechenzentrumskomponenten beziehen.

Diese Vorgehensweise hat auch die Behörde für Wissenschaft und Forschung (BWF) bei der Einführung des IT-Verfahrens zur Unterstützung der Verwaltungsprozesse, die bei der Beantragung der Sozialleistungen nach dem Bundes-Ausbildungsförderungs-Gesetz (BAföG) zu bearbeiten sind, gewählt. Im Berichtszeitraum sollte das seit langem produktive IT-Verfahren um eine Online-Komponente erweitert werden. Ziel dieser Komponente ist es, den Antragstellern eine Möglichkeit bereitzustellen, den Antrag auf dem eigenen PC auszufüllen und elektronisch an die zuständige Stelle zu senden. Da diese Erweiterung eine wesentliche Änderung des bestehenden Verfahrens darstellt, wurde von der Daten verarbeitenden Stelle eine ergänzende Risikoanalyse erstellt, in der zum einen der hohe Schutzbe-

darf der zu verarbeitenden Sozialdaten festgestellt wurde und andererseits die erforderlichen Schutzmaßnahmen festgeschrieben wurden. Bezüglich der funktionalen Erweiterungen besteht Einvernehmen, dass eine datenschutzgerechte Gestaltung gewählt wurde.

Aus Anlass der Erweiterung rückten jedoch auch noch einmal die beim IT-Dienstleister Dataport im Rechenzentrum genutzten Komponenten sowohl der Erweiterung als auch des BAföG-Vollverfahrens insgesamt in den Fokus. Auch die damalige Risikoanalyse des Vollverfahrens BAföG hatte das Ergebnis, dass ein hoher Schutzbedarf besteht. Dieser hohe Schutzbedarf hatte jedoch nicht dazu geführt, dass mit Dataport ein Service Level Agreement (SLA) bezüglich der Nutzung der Rechenzentrumskomponenten abgeschlossen worden ist, das diesem Schutzbedarf entsprach. Es war lediglich ein SLA auf der Grundlage des normalen Schutzbedarfs abgeschlossen worden. Weder dieser Tatbestand noch die damit verbundenen Risiken waren mit uns thematisiert oder in der Risikoanalyse offen gelegt worden.

Aufgrund unserer Nachfragen bei Dataport stellte sich kurz vor Redaktionsschluss heraus, dass nicht nur beim BAföG-Verfahren, sondern bei den meisten IT-Verfahren mit hohem Schutzbedarf, die von Dataport im Auftrag von Behörden der FHH betrieben werden, eine entsprechende Beauftragung nicht vorlag. Für die hamburgischen Behörden betreibt Dataport lediglich die produktiven Anwendungen ZIAF (für landwirtschaftliche Subventionen) und die Verfahren im DataCenter-Steuern sowie einige Infrastrukturkomponenten wie z. B. Exchange oder das HamburgGateway mit entsprechender expliziter Beauftragung eines hohen Schutzbedarfs. Bei den IT-Verfahren etwa aus dem Gesundheits- und Sozialbereich, den Verfahren der Polizei oder für die Unterstützung von Pass- und Meldeangelegenheiten erfolgte eine solche explizite Beauftragung durch die verantwortlichen Stellen nicht. Hier besteht dringender Handlungsbedarf.

Wir werden diese Erkenntnisse zum Anlass nehmen, gemeinsam mit der Finanzbehörde und Dataport die Schutzmaßnahmen im Rechenzentrum dahingehend zu betrachten, dass für IT-Verfahren mit hohem Schutzbedarf regelhaft zu treffende Maßnahmen definiert werden und weitere im Einzelfall zu beauftragende Module benannt werden. Ein erstes Gespräch hierzu hat erkennen lassen, dass eine solche Vorgehensweise von allen Beteiligten begrüßt wird. Ziel ist es auch, für solche Verfahren ein einheitliches Schutzniveau herzustellen, wie dies bei IT-Verfahren mit normalem Schutzbedarf bereits der Fall ist. Diese strukturierte Vorgehensweise soll die Daten verarbeitenden Stellen zukünftig besser in die Lage versetzen, ihrer Gesamtverantwortung gerecht zu werden.

III. DATENSCHUTZ IM ÖFFENTLICHEN BEREICH

1. Grundsatzfragen

1.1 Behördliche Datenschutzbeauftragte

Das Konzept des Senats zu Behördlichen Datenschutzbeauftragten hat zu einer erfreulichen Stärkung der Selbststeuerung nicht nur in den Kernbehörden, sondern auch bei vielen weiteren dem Hamburgischen Datenschutzgesetz unterliegenden Körperschaften geführt. In dieser Umbruchphase haben wir noch nicht alle unserer angekündigten Vorhaben umsetzen können, sondern zunächst verstärkt durch laufende Beratungen unsere Erfahrungen und Kenntnisse zur Verfügung gestellt.

Seit 2001 ermöglicht das Hamburgische Datenschutzgesetz (HmbDSG) mit § 10 a HmbDSG den Daten verarbeitenden Stellen, behördliche Datenschutzbeauftragte zu bestellen. Leider wurde davon in der Vergangenheit nur wenig Gebrauch gemacht (vgl. 21. TB, 3; 22. TB, III 1.1). Wir hatten deshalb wiederholt gefordert, die Kann-Bestimmung in eine Verpflichtung umzuwandeln. Zuletzt hatten wir von dem Vorhaben des Senats berichtet, die Kernbehörden anhand eines Konzepts verwaltungsintern zur Bestellung behördlicher Datenschutzbeauftragter zu verpflichten. Dieses Konzept ist am 01. Mai 2010 beschlossen worden. Erfreulicherweise haben bis Redaktionsschluss auf dieser Grundlage bis auf die Behörde für Inneres und Sport alle Senatsämter und Fachbehörden Beauftragte bestellt, von den 17 Gerichten bisher sieben und von den zwei Staatsanwaltschaften eine.

Besonders hervorzuheben ist, dass auch die Anzahl der Beauftragten bei den sonstigen Körperschaften des öffentlichen Rechts, die unserer Kontrolle unterliegen, deutlich gestiegen ist, unterliegen sie als eigenständige Körperschaften doch nicht der Weisungsbefugnis des Senats (z. B. Kammern, Innungen, Hamburg Port Authority, Hamburger Friedhöfe u. a.).

Mittlerweile haben alle staatlichen Hochschulen Beauftragte bestellt, wobei hier wie auch in der Bezirksverwaltung und bei den Gerichten von der Möglichkeit nach § 10 a Abs. 1 Satz 2 HmbDSG Gebrauch gemacht worden ist, eine Person für mehrere Stellen zu bestellen (sieben Hochschulen mit drei Beauftragten, sieben Bezirksämter mit einer Beauftragten und zwei Gerichte mit einer Beauftragten).

Nur selten haben die Behörden bisher die Möglichkeit genutzt, für verschiedene Bereiche mehrere Beauftragte zu bestellen. So verfügen bisher

in der Finanzbehörde die Steuerverwaltung und in der Behörde für Wissenschaft und Forschung die Staats- und Universitätsbibliothek über eigene Beauftragte.

Es bleibt zu wünschen, dass auch in der Behörde für Inneres und Sport, die insbesondere in den Bereichen Polizei, Verfassungsschutz und Ausländerwesen eine Vielzahl von unterschiedlichsten und sensiblen personenbezogenen Daten verarbeitet, alsbald eine entsprechende Bestellung erfolgt.

In der Sache hat sich unser Eindruck weiter bestätigt, dass die behördlichen Datenschutzbeauftragten einen erheblichen Gewinn für den materiellen Datenschutz bedeuten, werden sie vor Ort doch häufiger zu Einzelfragen und „Kleinigkeiten“ befragt und nicht erst mit den größeren Verfahren förmlich befasst. Ihre Sachnähe ermöglicht ihnen zudem oft schnellere Klärungen. Davon profitieren nicht zuletzt Petenten, die wir mit datenschutzrechtlichen Eingaben zunehmend an die behördlichen Datenschutzbeauftragten verweisen können. Hiermit sollte aber ein entsprechender Schutz bei den behördlichen Beauftragten verbunden sein. Zur Aufklärung von Defiziten sind Datenschutzbeauftragte auch auf entsprechende Hinweise angewiesen. Mitarbeiter der jeweiligen öffentlichen Stellen sollten deshalb schon nach dem äußeren Anschein sicher sein können, dass ihre Hinweise vertraulich bleiben. Wir haben daher gerade den Beauftragten, die noch andere fachliche Aufgaben wahrnehmen, empfohlen, auf Funktionspostfächer und entsprechend den Senatshinweisen auch auf eine offizielle Vertretung hinzuwirken.

Mit der Umsetzung des Konzepts wird zunehmend eine Verschiebung unserer Aufgabenschwerpunkte verbunden sein. Waren wir bisher u. a. mit der Eingabenbearbeitung und insbesondere der Vorabkontrolle einzelner automatisierter Verfahren befasst, so können daran gebundene Kapazitäten künftig verstärkt wieder für Prüfungen eingesetzt werden. Der Grad der Entlastung bleibt jedoch letztlich vom Einzelfall und vom Beratungsbedarf der einzelnen behördlichen Datenschutzbeauftragten abhängig. Zunächst gilt es aber, die Übergangszeit im Sinne eines möglichst kontinuierlichen Datenschutzes zu gestalten.

Dazu hatten wir in Aussicht gestellt, die behördlichen Datenschutzbeauftragten vielfältig in ihren Aufgaben durch regelmäßige halbjährliche Treffen, Austauschmöglichkeiten über einen Sharepoint und Fortbildungsangebote zu unterstützen.

Es hat sich gezeigt, dass diese Ziele mit den vorhandenen Kapazitäten im Berichtszeitraum nur bedingt erreicht werden konnten.

So haben wir Treffen bisher nur in annähernd jährlichen Abständen angeboten und zwei ganztägige Fortbildungen für neu bestellte Beauftragte durchgeführt. Dabei hatten wir wiederholt angeboten, auf kurzem Wege jederzeit unsere Erfahrungen und Kenntnisse abzufragen und Fragestellungen auch einzelfallbezogen gemeinsam zu erörtern. Es ist uns weiterhin wichtig, partnerschaftlich zur Realisierung des Datenschutzes beizutragen und nicht nur als Kontrollinstanz wahrgenommen zu werden.

Nachdem die Phase der Erstbestellungen nun weitgehend abgeschlossen ist, werden wir künftig verstärkt – auch angesichts der begrenzten zeitlichen Ressourcen der meisten Beauftragten – in Halbtagesveranstaltungen einzelne Themen zur vertieften Fortbildung anbieten.

Die Sharepoint-Lösung haben wir bisher aus kapazitären Gründen gänzlich zurückstellen müssen. Sie hat zusätzlich den Nachteil, dass darüber nur Beauftragte der Kernbehörden erreichbar sind. Einen laufenden Austausch aller Beauftragten auch zwischen den Treffen halten wir aber nach wie vor für erstrebenswert. Wir werden baldmöglichst Anstrengungen unternehmen, eine solche Kommunikationsplattform aufzubauen.

1.2 Videoüberwachung öffentlicher Stellen

1.2.1 Neue Regelung zur Videoüberwachung im Hamburgischen Datenschutzgesetz

Der neue § 30 des Hamburgischen Datenschutzgesetzes bildet die Querschnittsaufgaben der Videoüberwachung angemessen und verfassungskonform ab. Für eine rechtskonforme Anwendung kommt es auf eine sorgfältige Prüfung und Dokumentation der einzelnen Tatbestandsvoraussetzungen an.

Wir haben regelmäßig zu Fragen der Videoüberwachung berichtet, zuletzt zu den allgemeinen technischen und rechtlichen Anforderungen an eine verfassungskonforme Videoüberwachung (22.TB, II 5 und III 1.2).

Am 15. September 2010 ist der neue § 30 des Hamburgischen Datenschutzgesetzes (HmbDSG) in Kraft getreten, der als Querschnittsregelung die Videoüberwachung zu Hausrechtszwecken regelt. Dabei ist die Abstufung der Anforderungen an eine bloße Beobachtung und an eine Aufzeichnung zu begrüßen.

Leider ist der Gesetzgeber unserer Empfehlung nicht gefolgt, die Regelungen der §§ 8 und 9 HmbDSG für anwendbar zu erklären. Diese sehen bei automatisierten Verfahren zur Verarbeitung personenbezogener Daten eine dokumentierte Vorabkontrolle und eine allgemein verständliche Ver-

fahrensbeschreibung für alle Interessierten vor. Beide sind uns bzw. dem oder der bestellten Datenschutzbeauftragten vor Einführung zur Stellungnahme zuzuleiten.

Die in § 30 HmbDSG getroffene Vollregelungen zu den technischen Anforderungen und zur Dokumentation nehmen die dortigen Anforderungen nur unvollständig auf und erhöhen die Übersichtlichkeit nicht. Sie vermitteln die komplexen Abwägungsprozesse rechtlicher Art nur bedingt. Die zur Dokumentation erforderlichen Angaben zur Rechtmäßigkeit und Angemessenheit der Maßnahme nach § 30 Abs. 7 Nr. 6 HmbDSG erfordern folgende nacheinander vorzunehmenden Abwägungsschritte:

– Eine Beobachtung darf nur dann erfolgen, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Bestehen Anhaltspunkte, ist eine Beobachtung unzulässig. Dazu hat das Bundesverfassungsgericht u. a. betont, dass die Betroffenen grundsätzlich das Recht haben, sich frei und unbeobachtet in der Öffentlichkeit bewegen zu können.

– Eine Aufzeichnung darf erst dann erfolgen, wenn darüber hinaus Tatsachen die Annahme rechtfertigen, dass mit der Verletzung von Personen oder der Beschädigung von Sachen zu rechnen ist. Hierbei kann es sich nur um gewichtige Rechtspositionen handeln. Mit der Vorschrift ist jedenfalls keine Ausweitung der Haftung öffentlicher Stellen für das Eigentum Dritter verbunden.

– Schließlich müssen die getroffenen technischen und organisatorischen Maßnahmen in ihrer Gesamtheit geeignet und verhältnismäßig sein, bei einer nach den vorgenannten Maßstäben zulässigen Datenverarbeitung auch die Vertraulichkeit, Integrität, Verfügbarkeit und Revisionsfähigkeit der Daten sicherzustellen.

Alle diese Fragen sind bei Anlagen mit mehreren Kameras für jede einzelne Kamera zu beantworten. Denn die Überwachung muss den Bildausschnitt auf das erforderliche Maß beschränken und sie darf keine Bereiche erfassen, die ohne Not Auskunft über besonders sensitive Daten geben wie z. B. die Erfassung von Praxiseingängen oder Kirchen oder von Betroffenen auf Friedhöfen in ihrer Trauer.

Wir haben deshalb den Behörden im Herbst 2010 für die anspruchsvolle Dokumentation eine umfassende Handreichung und ein ausführliches Musterformular, das auch die erforderlichen Abwägungserfordernisse hinreichend darstellt, zur Verfügung gestellt.

1.2.2 Gesamterhebung Videoüberwachung

Die Gesamterhebung gestaltet sich als ein umfängliches und anspruchsvolles Verfahren, bei dem eine Vielzahl von Einzelfragen zu entscheiden sind. Die Abarbeitung kann deshalb nur sukzessive erfolgen. Es ist absehbar, dass nicht für alle Anlagen, die bisher zur Aufgabenwahrnehmung betrieben worden sind, eine tragfähige Rechtsgrundlage besteht.

Bisher hatten wir keine Kenntnis über die Anzahl der von öffentlichen Stellen im Sinne des §2 HmbDSG betriebenen und unserer Kontrolle unterliegenden Videoüberwachungsanlagen, da wir nicht in allen Fällen vor der Einführung zu beteiligen waren und in der Vergangenheit von den verantwortlichen Stellen nur in der Minderzahl der Fälle tatsächlich beteiligt wurden. Erste Angaben enthielten die Antworten des Senats auf Kleine Anfragen aus den Jahren 2009 und 2010 (zuletzt Drucksache 19/3945).

Wir haben deshalb die Novellierung des HmbDSG zum Anlass genommen, alle unserer Aufsicht unterstehenden öffentliche Stellen einschließlich der Beliehenen über die von ihnen unabhängig von der jeweiligen Rechtsgrundlage betriebenen Videoüberwachungsanlagen zu befragen. Aus Rechtsgründen zählten hierzu nicht die dem HVV angehörenden Unternehmen und die seit dem 01.01.2011 der alleinigen Aufsicht durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unterstehenden Dienststellen der team.arbeit Hamburg.

Da die Erhebung eine Prüfung im schriftlichen Verfahren ermöglichen sollte, haben wir dazu einen ausführlichen Fragebogen pro Videoanlage und je ein Blatt Anlage pro Kamera entwickelt und um aussagefähige Fotos vom tatsächlichen Aufnahmewinkel und möglichen Maximaleinstellungen gebeten. Wir haben die Stellen darauf hingewiesen, dass wir zunächst schwerpunktmäßig die nach Hausrecht betriebenen Anlagen prüfen wollten.

Das Antwortverhalten war sehr unterschiedlich. Gerade die Hamburg Port Authority (HPA) mit den mit Abstand meisten gemeldeten Anlagen hat umfassend und fristgerecht geliefert. Viele Stellen antworteten jedoch unvollständig, teilweise offenbar ohne nähere rechtliche Prüfung oder auch verspätet, wobei die Behörde für Inneres und Sport sich erst nach einem längeren Schriftwechsel nach Fristablauf zur Beantwortung der von uns gestellten Fragen bereit erklärt hat und die große Anzahl der polizeilichen Anlagen erst jetzt sukzessive nachliefert.

Insgesamt sind 463 Stellen (Behördenleitungen, Gerichte, Körperschaften und Beliehene) befragt worden.

Davon haben 420 Fehlanzeige gemeldet (keine Anlagen, Unzuständigkeit, Auflösung).

Von den 43 Betreibern wurden insgesamt 110 Anlagen mit 1147 Kameras und einer Attrappe gemeldet.

24 Behörden (Senatsämter, Behörden, Gerichte, Senats- und Bürgerschaftskanzlei) haben 52 Anlagen mit 802 Kameras gemeldet, davon allein 521 im Justizvollzugsbereich.

18 Körperschaften des öffentlichen Rechts haben 57 Anlagen mit 344 Kameras gemeldet, davon allein 195 bei der HPA.

Von den Beliehenen wurde eine Kamera-Attrappe gemeldet.

Die erste Sichtung der Unterlagen ergab folgendes Bild:

Die Videoüberwachung wird vielfältig eingesetzt. Anders als das BDSG kennt § 30 HmbDSG jedoch nicht die Videoüberwachung zur Aufgabenwahrnehmung. In vielen klassisch gewachsenen Bereichen muss die Videoüberwachung deshalb intensiv geprüft werden.

Aber auch die dem Hausrecht unterliegenden Fälle sind nach der Rechtsprechung des Bundesverfassungsgerichts oft kritischer zu würdigen als dies bisher erfolgt ist.

Abgrenzungsfragen ergeben sich etwa hinsichtlich der sog. Übersichtsaufnahmen. Wurde früher oft vertreten, solche Aufnahmen seien ohne datenschutzrechtliche Relevanz, so muss heute unter Beachtung der Rechtsprechung des Bundesverfassungsgerichts und der technischen Möglichkeiten aller zusammenwirkenden Komponenten einer Anlage geklärt werden, ob sichergestellt ist, dass die Technik tatsächlich nicht mehr als Übersichtsaufnahmen in zulässigem Umfang ohne personenbeziehbare Daten erstellen kann.

Sog. Blackbox-Verfahren sind erst dann zulässig, wenn sie die rechtlichen Anforderungen an Videoaufzeichnungen erfüllen.

Wir haben weitere typische Rechtsfragen wie die Grenzen des Hausrechts, z. B. bei Fried- und Betriebshöfen, die Beauftragung von Wachunternehmen sowie die Frage behandelt, welche Maßstäbe für eine Teilnahme öffentlicher Stellen am Wettbewerb anzulegen sind. Auf dieser Grundlage haben wir angefangen, die Anlagen nach Fallgruppen abzuarbeiten und zunächst die Klingelanlagen mit Videoüberwachung betrachtet.

Die Sachbearbeitung der einzelnen Anlagen wird angesichts der Vielfältigkeit, des Umfangs und der vorhandenen Kapazitäten nur sukzessive erfol-

gen können. Letztlich setzten bisher auch die personellen Engpässe der Dienststelle insoweit einer zügigen Prüfung Grenzen.

Mit den in einer Vielzahl von Fällen gestellten Nachfragen und der Nachforderung von Unterlagen, soll festgestellt werden, ob die Anlagen nach Aktenlage keine wesentlichen Anhaltspunkte für datenschutzrechtliche Bedenken bieten.

Die Ergebnisse sollen den Daten verarbeitenden Stellen, nach Fallgruppen zusammengestellt und zu Handlungsempfehlungen zusammengefasst, zur Verfügung gestellt werden.

Soweit eine Vielzahl der zur Zeit betriebenen Anlagen letztlich der Sicherheit des Verkehrs dienen (Elbtunnel, Brücken, Schleusen) und hinreichend bestimmte bundesrechtliche Regelungen bisher nicht getroffen worden sind, haben wir eine bundesweite Diskussion des Themas unter den Datenschutzbeauftragten des Bundes und der Länder angeregt.

Wir werden über den Fortgang der Aktion berichten.

2. Personaldaten

2.1 ePers/KoPers

Die Nutzung der Produktivdaten für die Entwicklung des IT-Verfahrens konnte verhindert werden.

Nach Abschluss des Kooperationsvertrages zur Neuausrichtung der IT-Unterstützung von Personalmanagementaufgaben in der Freien und Hansestadt Hamburg sowie in Schleswig-Holstein (vgl. 22. TB III 2.1) hatte Dataport das Vergabeverfahren im März 2010 eingeleitet. Im April 2011 erteilte Dataport den Zuschlag der Wiesbadener P&I Personal & Informatik AG.

Der Auftragnehmer hat im Rahmen seiner Vorstellung über das weitere Vorgehen die Anforderung definiert, zur Initialisierung ihres Personalmanagementsystems die Personalstammdaten sowie die Abrechnungsergebnisse sämtlicher Beschäftigter bei der FHH zu benötigen. Mit dem Projekt KoPers war daher zu erörtern, welche Möglichkeiten der Bereitstellung dieser personenbezogenen Daten nach dem HmbDSG für den Auftragnehmer bestehen. Aus datenschutzrechtlicher Sicht kommt in dieser ersten Phase ausschließlich eine anonymisierte Bereitstellung in Betracht, wobei diese Daten das Rechenzentrum von Dataport nicht verlassen und der Zugriff nur unter definierten Bedingungen erfolgt. Aus diesem Grund wurden Datenfelder aus dem für die Entwicklung nutzbaren Datenbestand entfernt, die einen Rückschluss auf die Person ermöglichen.

Parallel entwickelt das Projekt ePers mit den Behörden auf Basis der Software des Auftragnehmers die Eckpunkte für ein Bewerbermanagementverfahren, das bereits im Frühjahr 2012 in den Echtbetrieb gehen soll. Erste Entwürfe für eine Verfahrensbeschreibung und Risikoanalyse wurden mit uns erörtert.

Die Lenkungsgruppe ePers hatte am 14.11.2011 beschlossen, dass die datenschutzrechtlichen Fragen zwischen dem Projekt und uns abgestimmt werden. Die Unterrichtung der behördlichen Datenschutzbeauftragten erfolgt kontinuierlich durch die jeweils datenverarbeitenden Stellen. Es besteht Einvernehmen, dass das Projekt die notwendigen Verfahrensbeschreibungen und Risikoanalysen für die Daten verarbeitenden Stellen erstellt.

3. Polizei

3.1 Gesetzentwurf zur Polizeirechtsmodernisierung mit Licht und Schatten

Die notwendige Anpassung des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) an die Rechtsprechung des Bundesverfassungsgerichts wird begrüßt; gleichwohl sind einige Neuerungen des Gesetzentwurfs kritisch zu sehen.

Die von der Behörde für Inneres und Sport (BIS) vorbereitete Novelle des PolDVG (PolDVG-E; vgl. Bürgerschafts-Drs. 20/1923) enthält rechtsstaatlich erforderliche Anpassungen des geltenden Rechts an die Rechtsprechung des Bundesverfassungsgerichts, deren Umsetzung begrüßt wird. Dies gilt insbesondere für eine weitgehend durchgängige Implementierung von Vorschriften zum Schutz des Kernbereichs privater Lebensgestaltung im Rahmen bestehender Eingriffsregelungen (vgl. bereits 21.TB 8.1, 22. TB III. 4.1). Gleichzeitig darf jedoch nicht verkannt werden, dass die Neuregelungen künftig die Hürden für staatliche Eingriffe in die Grundrechte absenken werden. Der Polizei werden durch die Novelle zusätzliche und teilweise erweiterte Befugnisse für die Überwachung von Bürgerinnen und Bürgern eingeräumt.

Aus den Grundrechten sowie der Rechtsprechung des Bundesverfassungsgerichts, die diese interpretiert und ausformt, ergeben sich zum Teil detaillierte Zulässigkeitsgrenzen für polizeiliche Eingriffsnormen. Eine Orientierung hieran führt jedoch nicht zwangsläufig zu Gesetzen, die einen aus der Sicht des Datenschutzes in jedem Fall gelungenen Ausgleich zwischen Sicherheitsinteressen des Staates und den Bürgerrechten herstellen. Unsere Bewertung des Entwurfs, die wir der Behörde für Inneres

und Sport vor der Befassung des Senats mitgeteilt haben, orientierte sich daher nicht nur am Mindestmaßstab des rechtlich Zulässigen, sondern beinhaltete darüber hinaus auch Vorschläge, die aus Sicht des Datenschutzes im Rahmen der Polizeirechtsnovelle insgesamt geboten erscheinen.

Die zahlreichen detaillierten Änderungen des Entwurfs erschweren den Überblick über den Gesamtinhalt der teilweise neu gefassten Normen. Im Umgang mit dem zukünftig geänderten Gesetzestext ist bei Auslegungsfragen jeweils im Einzelnen zu entscheiden, welche Sätze des Begründungstextes der vorigen Fassung nach der jetzigen Änderung noch gelten und welche Passagen hinfällig geworden sind.

Für die Transparenz und Verständlichkeit des Entwurfstextes erweisen sich die zahlreichen Verweisungen als hinderlich. Wir hätten es bevorzugt, wenn anstelle der unterschiedlichen und komplexen Verweisungsnormen (z. B. § 10 Abs. 2 Satz 1, § 10a Abs. 2 und Abs. 5 Satz 6 und Abs. 7 Satz 6, aber auch z. B. § 10d Abs. 1, § 10e Abs. 4 und 5 PolDVG-E) der vollständige Regelungswortlaut in die jeweiligen Normen aufgenommen worden wäre. Zwar werden die einzelnen Normen dadurch länger. Die Verständlichkeit der Gesetze für die Bürgerinnen und Bürger, aber auch für die Vollzugsbehörden selbst, ist jedoch eine zentrale Voraussetzung für deren soziale Wirksamkeit und rechtsstaatlich sichere Anwendung. Im Übrigen ist das Bemühen, im Entwurf zur Verbesserung der Transparenz unterschiedliche Eingriffsbefugnisse und Maßnahmen in verschiedenen Normen zu regeln, zu begrüßen. Dies gilt insbesondere für die übersichtliche Struktur der verdeckten Überwachungsmaßnahmen in §§ 9 bis 10f PolDVG-E.

Bedenklich ist die Streichung des die Eingriffsbefugnisse bislang begrenzenden Kriteriums der „unmittelbar bevorstehenden Gefahr“ an verschiedenen Stellen des Gesetzentwurfs (so zum Beispiel in § 9 Abs. 1 Satz 1 Nr. 1, § 10a Abs. 1 Satz 1, § 12 Abs. 1 Satz 1 Nr. 1 PolDVG-E, § 16 Abs. 2 Nr. 4 des Änderungsentwurfs zum Hamburgischen Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung – SOG-E –). Das Erfordernis des Vorliegens einer zeitlich nahen Gefahrenlage hat sich bislang als ein begrenzendes Korrektiv staatlichen Eingriffshandelns erwiesen, dessen Verzicht im Einzelfall einer besonderen Prüfung zu unterziehen ist und einer besonderen Begründung bedarf. Bedauerlicherweise hat sich die Behörde für Inneres und Sport unseren Vorschlägen nicht anzuschließen vermocht.

Andererseits ist zu begrüßen, dass an der zunächst vorgesehenen Ermächtigung zur heimlichen Wohnungsdurchsuchung, die dazu dienen sollte, um auf diese Weise im Rahmen der neu eingeführten Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) heimlich Überwachungs-

Software auf informationstechnische Systeme von Störern aufzuspielen (§ 10f PolDVG-E), nicht mehr festgehalten wird. Bezüglich der Vereinbarkeit einer heimlichen Wohnungsdurchsuchung mit dem Grundrecht auf Unverletzlichkeit der Wohnung nach Art. 13 GG bestanden unsererseits erhebliche verfassungsrechtliche Bedenken. Ferner wurde die Eingriffsschwelle für einen präventiven Lauschangriff in § 10a Abs.1 Satz 1 PolDVG-E auf eine „dringende" Gefahr erhöht. Zudem wurde klargestellt, dass die verfahrenssichernden Maßnahmen auch für die Quellen-TKÜ gelten sollen, was unserer Ansicht nach im Entwurf zunächst nicht hinreichend deutlich geworden war. Wir halten dies für wichtig, da verfahrensrechtliche Anforderungen unmittelbar dem Grundrechtsschutz Betroffener dienen.

In einigen Punkten konnten wir unsere Auffassung leider nicht durchsetzen und sehen hier weiterhin bedenkliche Regelungen: So hätten wir uns eine Klarstellung gewünscht, dass vor einer Videoüberwachung nach § 8 PolDVG eine Risikoanalyse sowie eine Verfahrensbeschreibung gemäß §§ 8 Absatz 4 und § 9 des Hamburgischen Datenschutzgesetzes anzufertigen sind. Ferner ist die Vorschrift zur polizeilichen Videoüberwachung öffentlicher Plätze nach § 8 Absatz 3 PolDVG immer noch nicht hinreichend konkretisiert. Die Anforderung, dass diese Maßnahme nur an Kriminalitätsschwerpunkten eingesetzt werden darf, wäre sinnvoll gewesen. Wir hätten uns eine Verlagerung der Zuständigkeit beim Richtervorbehalt gewünscht. Nach momentaner Gesetzeslage ist hierfür das Amtsgericht zuständig. Wir halten eine Zuständigkeit des Hamburgischen Oberverwaltungsgerichts für zielführender, weil Hauptsacheverfahren, in denen sich Betroffene gerichtlich gegen verdeckte (gefahrenabwehrrechtliche und Straftaten verhütende) Überwachungsmaßnahmen zur Wehr setzen, vor der Verwaltungsgerichtsbarkeit geführt werden. Außerdem handelt es sich bei den verdeckten Überwachungsmaßnahmen um schwerwiegende Grundrechtseingriffe, so dass das anordnende Gericht über spezifische Verwaltungs- und Verfassungsrechtskenntnisse verfügen sollte und dem schwerwiegenden Grundrechtseingriff durch die Zuständigkeit eines hochrangigen Kollegialgerichts besonders Rechnung tragen würde (in diesem Sinne § 29 Abs. 6, §§ 31 ff. Polizei- und Ordnungsgesetz Rheinland-Pfalz, wonach das Oberverwaltungsgericht Koblenz zuständig ist).

Beim neu geregelten KfZ-Kennzeichenscanning nach § 8a PolDVG-E halten wir das Verbot nicht näher definierter „Bewegungsprofile" für nicht ausreichend. Leider hat die BIS die von uns vorgeschlagene Definition zum Verbot einer langfristigen Observation nicht in den Gesetzesentwurf aufgenommen.

Bei der Kritik an den ausgeweiteten Möglichkeiten einer zwangsweisen Vorführung, die bisher nur zur Abwehr einer Lebensgefahr zulässig war und nach § 11 Abs. 3 Nr. 1 SOG-E bereits zulässig sein soll, wenn die Angaben der betroffenen Person zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person erforderlich sind, konnten wir uns mit unseren Bedenken nicht durchsetzen. Die Hamburgische Regelung fällt hier im Vergleich zu entsprechenden Regelungen in anderen Bundesländern zurück, (vgl. etwa § 10 Abs. 3 PolG NRW, § 15 Abs. 3 BbgPolG, § 35 Abs. 4 SOG LSA, § 19 Abs. 1 NdsSOG, § 51 Abs. 1 und 3 MV SOG), denn sie steht nicht unter dem Vorbehalt der richterlichen Anordnung. Dies wäre daher zur verfahrensmäßigen Absicherung der Rechte Betroffener zumindest wünschenswert gewesen.

Die herabgesetzte Eingriffsschwelle in § 11 Abs. 3 Nr. 1 SOG-E führt durch die Bezugnahme in § 16 Abs. 2 Nr. 1 SOG-E unweigerlich zu einer Ausweitung des Anwendungsbereichs der Vorschrift über das Betreten und Durchsuchen von Wohnungen. Eine Ausweitung der Kompetenz der Wohnungsdurchsuchung muss mit Blick auf das Grundrecht in Art. 13 Grundgesetz (GG) kritisch gesehen werden. Das gilt insbesondere vor dem Hintergrund, dass die Anordnung von erkennungsdienstlichen Maßnahmen, für die eine Vorladung nach § 11 Abs. 3 SOG-E möglich ist, aus unterschiedlichen Gründen erfolgen kann.

3.2 Videoüberwachung Reeperbahn

Inzwischen wurde die Videoüberwachung der Reeperbahn von der Polizei Hamburg eingestellt. In ihrer Wirksamkeitsanalyse kommt die Polizei zu dem Schluss, dass einige Indizien für eine Wirksamkeit der Videoüberwachung sprächen; das Hamburgische Oberverwaltungsgericht hält die Überwachung von Eingangsbereichen für rechtswidrig.

Über die polizeiliche Videoüberwachung öffentlicher Plätze hatten wir bereits in den vorangegangenen Jahren berichtet (21. TB, 8.2; 22. TB, III 4.4). Wir hatten unter anderem kritisiert, dass die Wirksamkeitsanalyse zur Unterrichtung der Bürgerschaft über die Auswirkungen der Videoüberwachung der Reeperbahn, behördenintern erstellt werden sollte; sie erfüllt damit nicht die nach unserer Auffassung an eine unabhängige und wissenschaftlich fundierte Evaluierung zu stellenden Anforderungen. Diese Kritik besteht unverändert fort, nachdem der Senat in der Drucksache 19/6679 vom 06.07.2010 die „Unterrichtung der Bürgerschaft über die Videoüberwachung der Reeperbahn (Wirksamkeitsanalyse)“ vorgenommen hat. U. a. durch eine Kombination der Videoüberwachung mit anderen polizeilichen Maßnahmen, wie beispielsweise einer erhöhten Polizeipräsenz im

überwachten Bereich, ließ sich letztlich keine Aussage dazu treffen, welche Auswirkung die Videoüberwachung auf die Kriminalitätsentwicklung hatte. Zudem stieg die Kriminalitätsrate in einigen Bereichen, während sie in anderen Bereichen sank; über die Ursachen kann nur spekuliert werden. Das Ziel der Reduzierung des Fallaufkommens insgesamt in dem Bereich der Reeperbahn sei in den ersten drei Jahren der Überwachung nicht erreicht worden. Allerdings betont der Senat, dass durch die Videoüberwachung die Aufklärung von Straftaten erleichtert worden sei. Für die Durchführung einer Videoüberwachung zum Zweck der Strafverfolgungsvorsorge ist die Kompetenz des Hamburgischen Gesetzgebers, dies landesrechtlich im Gesetz über die Datenverarbeitung der Polizei (PolDVG) zu regeln, zweifelhaft.

In seinem Urteil vom 22.06.2010 (4 Bf 276/07) hält das Hamburgische Oberverwaltungsgericht die Regelung des § 8 Absatz 3 PolDVG insgesamt für verfassungsmäßig. Zugrunde lag die Klage einer Anwohnerin der Reeperbahn, die sich gegen die Beobachtung ihrer Wohnung und des dazugehörigen Hauseingangsbereichs wendete. Das Hamburgische Oberverwaltungsgericht hält die Gesetzgebungskompetenz des Landesparlaments zur Videoüberwachung zum Zweck der Strafverfolgungsvorsorge für gegeben. Allerdings hat das Bundesverwaltungsgericht mit Beschluss vom 28.3.2011 (BVerwG 6 B 56.10) die Revision der Klägerin zugelassen, um zur Klärung dieser strittigen Fragen beizutragen, ob die offene Bildaufzeichnung im öffentlichen Raum zum Zwecke der Strafverfolgungsvorsorge auf das Polizeigesetz eines Bundeslandes gestützt werden darf oder ob die Gesetzgebung des Bundes zum Strafverfahrensrecht insoweit abschließend ist.

Trotz der grundsätzlichen verfassungsrechtlichen Zulässigkeit beschränkt das Hamburgische Oberverwaltungsgericht die Auslegung des Begriffs der „öffentlich zugänglichen Orte“ in § 8 Abs. 3 PolDVG auf öffentlich zugängliche Straßen, Wege und Plätze. Ausdrücklich nimmt es andere (anliegende, öffentliche, private) Flächen bzw. Gebäude, auch soweit diese öffentlich zugänglich sind, und damit auch Eingangsbereiche zu Gebäuden, aus. Das Gericht führt dazu aus: „Der Eingriff ist hier noch intensiver als bei der Videoüberwachung des öffentlichen Straßenraums. Denn mit dem Hauseingang ist der Übergang zum Privatbereich der Klägerin betroffen. Durch die in Streit stehende Videokamera werden Bildübertragungen und -aufzeichnungen sowohl des inneren als auch des äußeren Hauseingangsbereichs vorgenommen. Auf diese Weise kann ohne weiteres ein Bewegungs- und Besuchsprofil der Klägerin erstellt werden.“

Die Polizei sah sich nach dem Urteil gezwungen, praktisch alle Gebäude – samt Eingangsbereichen – von der Videoüberwachung durch eine Unkenntlichmachung der jeweiligen Bildausschnitte auszunehmen. Mit der früheren Kameratechnik, die eine Schwarzschaltung des Bildschirms bewirkte, sobald ein „verbotener" Bereich angesteuert wurde, wäre eine Videoüberwachung der Reeperbahn nicht mehr möglich gewesen. Mit einer neuen Technik sollten „verbotene" Flächen dadurch von der Beobachtung ausgenommen werden, dass diese Bereiche von Polygonen überlagert und damit nicht zu sehen sind, während auf dem Bildschirm alle erlaubten Bereiche ohne Beeinträchtigung erkennbar bleiben. Die Polygon-Technik erlaubt eine feinere Ausblendung von Flächen, die nicht beobachtet werden sollen, erschwerte aber dennoch die Videoüberwachung für die jeweils beobachtenden Polizeibediensteten.

Die durch das Urteil notwendig gewordenen Umstellungen gaben für die Polizei Veranlassung, Erkenntnisgewinn und Aufwand der Videoüberwachung neu zu überprüfen. Die Abwägung führte im Juli 2011 zu der Entscheidung, die dauerhafte Videoüberwachung der Reeperbahn einzustellen.

3.3 Minderheitengruppenzugehörigkeit in der Polizeistatistik

Eine datenschutzrechtliche Überprüfung der Nennung von Minderheitengruppen im Zusammenhang mit statistischen Angaben über Wohnungseinbrüche ergab zwar keine Anhaltspunkte für einen Personenbezug. Im Kern wirft die Thematik jedoch diskriminierungsspezifische Fragen auf. Angaben über die Zugehörigkeit zu Minderheiten gehören nicht in behördliche Statistiken.

Im Mai 2010 bat uns der Zentralrat Deutscher Sinti und Roma, die Zulässigkeit des Speicherns von Minderheitenzugehörigkeit zu den Volksgruppen der Sinti und Roma im Rahmen von statistischen Angaben zu überprüfen. Anlass war ein Zeitungsartikel, in dem ein Polizeisprecher dahin gehend zitiert wurde, dass die deutlich gestiegene Zahl der Wohnungseinbrüche vor allem auf Täter aus dem „Milieu der Sinti und Roma" zurückzuführen sei.

Wir haben daraufhin bei der Polizei Hamburg überprüft, ob die Daten in den Statistiken einen Personenbezug aufweisen. Nur unter diesen Voraussetzungen kann der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit tätig werden.

In den Strukturermittlungsdateien über Wohnungseinbrüche waren keine personenbezogenen Angaben über die Gruppenzugehörigkeit von Sinti

und Roma gespeichert. Lediglich in einer internen Controllingliste der allerdings nur vorübergehend eingesetzten Sonderermittlungsgruppe zu Haus- und Wohnungseinbrüchen, die banden- oder gewerbsmäßig begangen wurden, wurden das Gruppenzugehörigkeitsmerkmal „Sinti und Roma“, aber auch andere Gruppenzugehörigkeiten, wie z. B. Nationalitäten oder Volksgruppenzugehörigkeiten, eingetragen. Die Angaben in dieser Statistik wiesen ebenfalls keinen Bezug zu einzelnen Personen auf. Die Eintragungen der Merkmale in die Listen erfolgten durch die zuständigen Sachbearbeiter der Ermittlungsgruppe in anonymisierter Form jeweils dann, wenn ein Zeuge nach Mutmaßungen einen Verdächtigen der Minderheit der Sinti und Roma zugeordnet hatte. Mangels eines Personenbezugs der Statistik mussten wir dem Vorsitzenden des Zentralrats Deutscher Sinti und Roma mitteilen, dass wir datenschutzrechtlich den Sachverhalt nicht weiter verfolgen konnten.

Jenseits der isolierten datenschutzrechtlichen Betrachtung sei angemerkt, dass es einen äußeren Anschein einer Volksgruppenzugehörigkeit nicht gibt und die Zuordnung letztlich auf bloßer Mutmaßung durch Zeugen beruht. Die Verwendung von Minderheitsbezeichnungen in einem behördlichen Auskunftssystem oder in einer Statistik entfaltet auch ohne einen individuellen Bezug durchaus diskriminierende Wirkungen für die Angehörigen der jeweiligen Minderheit. Hierdurch besteht die Gefahr, dass diese quasi unter Generalverdacht gestellt wird.

Wir gehen davon aus, dass durch die Anfrage und unsere Nachforschungen der sensible Blick auf die Diskriminierungsproblematik von Angaben zur Minderheitenzugehörigkeit geschärft werden konnte.

3.4 Videoüberwachung einer angemeldeten studentischen Versammlung

Finden angemeldete Versammlungen statt, so dürfen auch nicht zu anderen Zwecken vorgehaltene Kameras dazu eingesetzt werden, Teilnehmer einer Versammlung in Ausübung ihres Grundrechts zu beobachten, wenn nicht tatsächliche Anhaltspunkte für eine erhebliche Gefahr für die Sicherheit und Ordnung ausgehen.

Durch eine Eingabe wurden wir nachrichtlich darüber informiert, dass die Veranstalter des Protestcamps „Alternative Uni“ im Sommer 2010 im Rahmen eines verwaltungsgerichtlichen Eilverfahrens die Änderung einer Kameraeinstellung erwirkt hatten.

Die Kamera war von der Polizei ursprünglich zu Zwecken der Verkehrsüberwachung angebracht worden. Während der Protestveranstaltung wurde

sie aus Anlass einer vermuteten Gefahr jedoch auf das Protestcamp gerichtet und in dieser Position belassen.

Die Polizei hatte sich bereits in ihrer Stellungnahme gegenüber dem Verwaltungsgericht dahingehend eingelassen, dass die Kameraeinstellung so geändert worden sei, dass sie die Veranstaltung nicht mehr erfasste.

Im Rahmen einer hierzu parallel gestellten Kleinen Anfrage an den Senat hatten wir festgestellt, dass eine Videoüberwachung nur zulässig sei, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass von den Teilnehmern bei oder im Zusammenhang mit öffentlichen Versammlungen erhebliche Gefahren für die Sicherheit und Ordnung ausgingen.

In einer späteren Stellungnahme hat uns die Rechtsabteilung der Polizei bestätigt, dass das Wegdrehen der Kamera unverzüglich nach der Erkenntnis erfolgte, dass sie auf den Ort der Versammlung gerichtet war, dort aber keine Gefahrenlage im Sinne der von uns zitierten Vorschriften und der Rechtsprechung des Bundesverfassungsgerichts zu Übersichtsaufnahmen anlässlich von Versammlungen mehr bestand. Die zuständigen Beamten seien anlässlich dieses Vorfalls bezüglich der Rechtslage sensibilisiert worden.

4. Verfassungsschutz

4.1 Auskunfts- und Löschungspraxis des Landesamts für Verfassungsschutz

Quellenschutz und beschränkte Auskunftsrechte führen nur selten zur Löschung nicht (mehr) erforderlicher Erkenntnis-Daten im Landesamt für Verfassungsschutz (LfV).

Auch im Berichtszeitraum haben sich wieder Bürger an uns gewandt, weil sie mit der Antwort des LfV auf ihr Auskunftsbegehren nicht einverstanden waren.

Grundsätzlich besteht das datenschutzrechtliche Auskunftsrecht auch gegenüber dem LfV, § 23 HmbVerfSchG. Die Antworten des LfV, die uns von den Betroffenen vorgelegt wurden, zeugen davon, dass das LfV dieses Recht ernst nimmt. Im Unterschied zu anderen Landesämtern für Verfassungsschutz enthalten die Bescheide in Hamburg in der Regel konkrete Erkenntnisse (Mitgliedschaften, Teilnahme an Veranstaltungen extremer Organisationen usw.), die der Betroffene überprüfen kann.

Nach § 23 Abs.2 HmbVerfSchG „unterbleibt“ eine Auskunftserteilung des LfV jedoch, „soweit durch sie die Nachrichtenzugänge gefährdet sein können“. Diesen sog. Quellenschutz nimmt das LfV dann in Anspruch, wenn die anfragende Person durch eine Auskunft über die beim LfV vorliegenden Erkenntnisse Rückschlüsse auf mögliche Informanten ziehen könnte. Soweit die Auskunft in dieser Weise eingeschränkt wird, werden die Betroffenen darauf sowie nach § 18 Abs.6 HmbDSG auch darauf hingewiesen, dass sie sich an den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit wenden können. Wir prüfen dann vor Ort, welche Erkenntnisse gegen die betroffene Person vorliegen und ob der Quellenschutz zu Recht geltend gemacht wurde. In unserer Antwort an den Bürger teilen wir dann regelmäßig mit, dass entweder keine Anhaltspunkte für einen Datenschutzverstoß bestanden oder dass die Prüfung zu Erörterungen mit dem LfV geführt hat, über deren Ergebnis der Betroffene weitere Nachricht erhalten wird.

In einem Fall erschienen uns die nicht sehr aktuellen Erkenntnisse wenig belastbar. In Abstimmung mit dem LfV haben wir sie gegenüber der betroffenen Person weiter konkretisieren können, ohne den Quellenschutz zu verletzen. Dies hat dazu geführt, dass der Betroffene die Erkenntnisse in ihrem Wahrheitsgehalt bzw. ihrer aktuellen Gültigkeit vehement bestritt und eine sofortige Löschung verlangte. Das LfV hat die Erkenntnisse und Informanten noch einmal intensiv überprüft und uns dann mitgeteilt, dass alle zu der betroffenen Person gespeicherten Daten gelöscht würden.

Eine solche Reaktion des LfV ist selten. Die Tatsache, dass von Informanten mitgeteilte Anhaltspunkte für eine Unterstützung verfassungsfeindlicher Bestrebungen grundsätzlich nicht gerichtsfest bewiesen werden müssen, führt im Zweifel dazu, dass möglichst viele Erkenntnisse zu der Person gesammelt und in der Hoffnung auf zusätzliche Informationen auch längerfristig gespeichert werden. Insgesamt haben sich unsere Kooperation mit dem LfV und die Prüfung der jeweiligen Erkenntnislage vor Ort bewährt. Es ist zwar grundsätzlich nicht unsere Aufgabe, vorliegende Erkenntnisse auf ihre Eignung als Anhaltspunkte für verfassungsfeindliche Bestrebungen zu bewerten. Die hohe datenschutzrechtliche Bedeutung von LfV-Erkenntnissen z. B. für ausländerrechtliche und Einbürgerungsentscheidungen sowie die Einschränkung des Auskunftsrechts rechtfertigen es jedoch, dass wir die Belastbarkeit und Argumentationsstringenz der Erkenntnisse mit dem LfV erörtern und dabei das Recht auf informationelle Selbstbestimmung betonen.

5. Justiz

5.1 Elektronische Aufenthaltsüberwachung

Zur Aufenthaltsüberwachung von gefährlichen entlassenen Straftätern mithilfe der „elektronischen Fußfessel" hat sich Hamburg einem bundesweiten System angeschlossen. Der Datenschutz bei der Ausgestaltung und Umsetzung der Überwachung konnte gestärkt werden.

Seit Anfang 2011 kann ein Richter nach § 68 b Abs.1 Nr.12 StGB einem gefährlichen Strafentlassenen die Weisung erteilen, zur Überwachung seines Aufenthaltsortes eine technische Einrichtung (sog. „elektronische Fußfessel") zu tragen und funktionsfähig zu halten. § 463 a Strafprozessordnung erlaubt der Führungsaufsichtsstelle des jeweiligen Landes, die elektronischen Aufenthaltsdaten zu erheben und zu speichern. Diese Daten ergeben sich aus einer GPS-Ortung und dem Mobilfunknetz, wobei das Sendeintervall (z. B. alle 5 oder 15 Minuten) unterschiedlich sein kann. Die Daten dürfen verwendet werden, um einen Verstoß gegen richterliche Auflagen, bestimmte Orte nicht zu verlassen oder zu meiden (Ge- oder Verbotszonen), festzustellen und zu ahnden sowie um erhebliche gegenwärtige Gefahren abzuwehren. Ferner werden eine Zwei-Monatsfrist für die Datenlöschung sowie die Protokollierung von Datenzugriffen festgelegt. Die Normen schreiben aber nicht vor, dass die elektronische Aufenthaltsüberwachung sich nur auf (georeferenzierte und in die Software integrierte) Ge- oder Verbotszonen beziehen darf, also nur dann automatisiert einen Alarm auslöst, wenn diese Zonen verlassen bzw. betreten werden. Vielmehr soll die „flächendeckende" Aufenthaltsüberwachung dem Überwachten bewusst machen, dass er beobachtet wird und dass im Falle eines Rückfalls seine Anwesenheit in der Nähe des Tatorts nachzuweisen ist. Alarmmeldungen vor Betreten einer Verbotszone erfolgen aber nicht.

Im Februar 2011 hat uns die Justizbehörde über ihre Absicht informiert, die neuen rechtlichen Möglichkeiten in einem Verbundsystem mit den anderen Ländern und einer Datenzentrale in Hessen zu nutzen. Im März hat die Datenschutzkonferenz des Bundes und der Länder die Pläne behandelt. Zu den entsprechenden Entwürfen für einen Staatsvertrag und eine Verwaltungsvereinbarung haben wir ausführlich Stellung genommen. Wir haben u. a. die unklare Rechtsnatur der beteiligten hessischen Stellen und ihrer Zusammenarbeit kritisiert, Regelungen für die Kooperation mit der Polizei gefordert, auf Datenschutzprobleme bei der technischen Unterstützung vor Ort durch private Dienstleister hingewiesen und eine Beschränkung des Datenumfangs auf dem (Stamm-)Datenblatt für jeden Betroffenen angeregt.

Unsere Hinweise sind von anderen Landesdatenschutzbeauftragten übernommen und ergänzt und in den nachfolgenden Änderungen des Staatsvertrages und der Verwaltungsvereinbarung weitgehend berücksichtigt worden. Der Anfang Juni eingebrachten Senatsdrucksache der Justizbehörde zur Einführung der elektronischen Aufenthaltsüberwachung in Hamburg durch Abschluss der Verwaltungsvereinbarung und Beitritt zum Staatsvertrag haben wir deswegen zustimmen können.

Dennoch ist noch eine Reihe von datenschutzrechtlichen Details bei der elektronischen Aufenthaltsüberwachung und ihrer technisch-organisatorischen Umsetzung zu klären und verbindlich zu regeln. Eine Arbeitsgruppe des Strafrechtsausschusses der Justizministerkonferenz hat im August 2011 einen Entwurf zur Initiierung von Fallkonferenzen zur Vorbereitung der gerichtlichen Auflagen und Weisungen und zu weiteren Aspekten der richterlichen Entscheidung erarbeitet. Von datenschutzrechtlichem Interesse sind das von der Arbeitsgruppe entwickelte „Datenblatt Proband“ und die ins Einzelne gehenden „Handlungsanweisungen für die GÜL“ (Gemeinsame elektronische Überwachungsstelle der Länder) im hessischen Bad Vilbel. Die Führungsaufsichtsstellen der Länder übermitteln der GÜL die Betroffenendaten; die GÜL bedient sich für die technische Umsetzung der Überwachung der Hessischen Zentrale für Datenverarbeitung (HZD) (zum technischen Verfahren vgl. die Kleinen Parlamentarischen Anfragen 20/1388 und 20/1539).

Im Rahmen des Arbeitskreises Justiz der Datenschutzbeauftragten des Bundes und der Länder sowie bei konkreten Hamburger Einzelfällen werden wir die Entwicklung und Ausgestaltung der elektronischen Aufenthaltsüberwachung auch weiterhin begleiten und hierzu mit der Behörde für Justiz und Gleichstellung in Kontakt bleiben. Dies erscheint insbesondere deswegen geboten, weil die GÜL ihre Arbeit erst Anfang 2012 tatsächlich aufnimmt, während die HZD nur pseudonyme Daten verarbeiten soll.

5.2 Anerkennung ausländischer Scheidungsurteile

Für die Überprüfung ausländischer Scheidungsurteile fordert die Justizbehörde aufgrund unserer Anregungen nun nicht mehr die vollständige Ausländerakte an, sondern benennt die erforderlichen Unterlagen und Auskünfte anhand einer Ankreuzliste.

Aufgrund der Eingabe eines Bürgers haben wir uns mit der Praxis der Justizbehörde zur Anerkennung ausländischer Scheidungsurteile nach § 107 FamFG (Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit) zu befassen gehabt. Die Behörde forderte bislang nicht nur von der antragstellenden Person Unter-

lagen und Antworten zu einen umfangreichen Fragenkatalog an, sondern zusätzlich von der Ausländerbehörde die vollständige Ausländerakte. Zwar hat uns die Justizbehörde davon überzeugt, dass es nicht ausreicht, den Antragsteller auf seine Mitwirkungspflicht hinzuweisen und die Anerkennung bei fehlenden Angaben zu versagen: Zum einen ist von Amts wegen auch das Interesse des Ex-Ehepartners zu berücksichtigen, zum anderen ist die Antrag stellende Person oft auch bei gutem Willen faktisch nicht in der Lage, die erforderlichen Unterlagen beizubringen oder Auskünfte zu geben.

Wir haben aber deutlich gemacht, dass in einer Ausländerakte praktisch das gesamte Leben eines hier wohnhaften Ausländers dokumentiert ist – einschließlich sehr persönlicher Daten wie Gesundheits- und Familienverhältnisse. Für die Anerkennung eines ausländischen Scheidungsurteils sind dagegen in der Regel nur ganz bestimmte einzelne Dokumente und Fragen entscheidend. Die Übermittlung der gesamten Ausländerakte würde damit in der Mehrzahl Daten offenbaren, die für die Aufgabenerfüllung der Justizbehörde nicht erforderlich sind.

Um die Ausländerbehörde nicht mit einer Pflicht zur Auswahl der erforderlichen Dokumente aus der Ausländerakte zu überfordern – obwohl grundsätzlich den Datenübermittler die Pflicht zur Beschränkung der Datenoffenbarung auf das erforderliche Maß trifft –, haben wir uns mit der Justizbehörde auf folgendes Verfahren geeinigt:

Bei einem Antrag auf Anerkennung eines ausländischen Scheidungsurteils sendet die Justizbehörde der Ausländerbehörde ein Anforderungsschreiben mit dem Einleitungssatz: „Zur Prüfung der Angaben des Antragsstellers/der Antragstellerin und zur Entscheidungsfindung bittet die Behörde für Justiz und Gleichstellung unter Hinweis auf § 13 Abs.2 Nr.1, 2. Alt. HmbDSG, ihr Mehrfertigungen von Dokumenten aus der Ausländerakte (und Einbürgerungsakte) zu übersenden, soweit diese folgende Angaben enthalten….“ Es folgt eine Aufzählung von 60 möglichen Angaben, unter denen die Justizbehörde dann nur die im Einzelfall erforderlichen und gewünschten ankreuzt. Hinsichtlich weiterer Ankreuzfelder ohne inhaltliche Vorgabe haben wir darauf hingewiesen, dass hier nicht die gesamte Ausländerakte angefordert werden darf.

Ein gewisser Dissens ist bei der Auslegung des § 13 Abs.2 Nr.1, 2. Alternative HmbDSG verblieben. Nach dieser Norm ist eine weitere Datenverarbeitung (hier: Übermittlung durch die Ausländerbehörde) für andere Zwecke zulässig, wenn „die Wahrnehmung einer durch Gesetz oder Rechtsverordnung begründeten Aufgabe die Verarbeitung dieser Daten zwingend voraussetzt“. Es blieb offen, ob § 107 FamFG, der die Anerken-

nung ausländischer Scheidungen spezialgesetzlich regelt, durch bewussten Verzicht auf eine Datenverarbeitungsregelung die Datenübermittlung gerade verhindern will, statt sie „zwingend vorauszusetzen“. Wir haben dies nicht vertieft, da aus unserer Sicht das vereinbarte Verfahren im Ergebnis datenschutzrechtlich vertretbar und tragfähig ist.

5.3 Herausgabe von Tatortfotos an die Medien

Zur Wahrung des Persönlichkeitsrechts der Opfer können den Medien allzu drastische Tatortfotos der Staatsanwaltschaft vorenthalten werden.

Das NDR-Fernsehen wollte im Sommer 2011 noch einmal die blutigen Auseinandersetzungen im Hamburger Rotlichtmilieu in den 80er Jahren bearbeiten. Es bat die Staatsanwaltschaft um Tatort-, Opfer- und Täterfotos aus den Ermittlungsakten. Die Staatsanwaltschaft hatte jedoch Zweifel an einem entsprechenden Akteneinsichts- und Veröffentlichungsrecht der Medien. Sie hat uns deswegen unter Vorlage der ca. 30 in Betracht kommenden Fotos um eine Stellungnahme gebeten.

Wir haben die Rechtsauffassung der Staatsanwaltschaft geteilt, dass die Medien zwar grundsätzlich ein Informationsrecht nach § 4 Hamburgisches Pressegesetz haben, dass aber Auskünfte und Akteneinsichtnahmen verweigert werden können, wenn sie schutzwürdige private Interessen von Betroffenen verletzen würden. Aus Art.5 Grundgesetz (GG) lässt sich ein weitergehendes Akteneinsichtsrecht der Medien zu künstlerischen Zwecken nicht ableiten: Die Medien- und Darstellungsfreiheit von Presse, Rundfunk und Fernsehen „findet ihre Schranken in den Vorschriften der allgemeinen Gesetze“, Art. 5 Abs.2 GG. Es gelten deswegen die allgemeinen Vorschriften der §§ 474 ff. Strafprozessordnung (StPO) zur Akteneinsicht. Nach § 475 StPO sind Auskünfte und Akteneinsichtnahmen zu versagen, wenn Betroffene ein schutzwürdiges Interesse an der Versagung haben. Hier war zu berücksichtigen, dass die eingesehenen Fotos vom NDR gespeichert und veröffentlicht werden sollten.

Bei der Bewertung der Schutzwürdigkeit sind sehr verschiedene Gesichtspunkte zu berücksichtigen – die nach der Tat verstrichene Zeit ebenso wie ein besonderes Informationsinteresse der Bevölkerung, aber auch das Interesse Betroffener aus dem postmortalen Persönlichkeitsrecht an einer angemessenen Darstellung. Je deutlicher das Gesicht des Opfers zu identifizieren ist, je entstellter das dargestellte Opfer erscheint und je spektakulärer die wiedergegebenen Begleitumstände, desto eher könnten mit der Herausgabe und Veröffentlichung der Fotos schutzwürdige Interessen der Betroffenen verletzt werden. Auch bei Täterfotos gibt es Grenzen der Aus-

kunft und Herausgabe – etwa, wenn neben Portraitfotos auch Bilder mit entblößtem Körper veröffentlicht werden sollen.

In einer gemeinsamen Bewertung nach den vorstehenden Kriterien haben Staatsanwaltschaft und wir eine (kleine) Zahl von Fotos ausgewählt, die dem NDR nicht zur Verfügung zu stellen waren. Aufgrund der unterschiedlichsten höchstrichterlichen Urteile zum Persönlichkeitsschutz ist uns aber bewusst, dass solche Auswahlentscheidungen nicht ohne subjektive und situationsbedingte Beurteilungselemente auskommen. Solche Abwägungen sind aber ein im Datenschutzrecht häufig wiederkehrendes Instrument, trotz widerstreitender Interessen zu einer Entscheidung zu kommen.

5.4 Rechtsanwaltskammer

Als öffentliche Stelle bedarf auch die Rechtsanwaltskammer für die Verarbeitung personenbezogener Mitgliederdaten spezialgesetzlicher Befugnisnormen.

Ein Rechtsanwalt bat uns, bei der Kammer die Vernichtung einer gerichtlichen Mitteilung über eine Zivilklage gegen ihn durchzusetzen. Solche Mitteilungen sind nach § 36 a Bundesrechtsanwaltsordnung (BRAO) und der Anordnung über Mitteilungen in Zivilsachen (MiZi) vorgesehen, damit die Kammer z. B. den drohenden Vermögensverfall eines Rechtsanwalts rechtzeitig erkennen und ggf. Schritte einleiten kann. Obwohl die Gerichte nach § 20 Einführungsgesetz zum Gerichtsverfassungsgesetz (EGGVG) immer auch den Ausgang des Verfahrens mitzuteilen haben, wird dies in der Praxis häufig versäumt. Im Einzelfall enthält die Mitgliederakte dann zu Unrecht nur negative Angaben.

In einem persönlichen Gespräch mit dem Kammervorstand sind wir übereingekommen, dass die Kammer jede gerichtliche Mitteilung zunächst daraufhin überprüft, ob sie überhaupt für eine Aufsichtsmaßnahme der Kammer in Betracht kommen kann. Jedenfalls vor einer Maßnahme gegen das Mitglied wird sie ggf. auch eine (versäumte) Mitteilung über den Verfahrensausgang anfordern, ohne die eine angemessene Beurteilung des Sachverhalts nicht möglich ist. Im Übrigen haben wir zugestanden, dass zunächst auch solche Mitteilungen aufbewahrt werden, die zwar nicht für sich allein, doch zusammen mit anderen Mitteilungen ein Tätigwerden der Kammer rechtfertigen können. Auf einen entsprechenden Antrag des betroffenen Mitglieds überprüft die Kammer, ob eine weitere Speicherung der Mitteilungen noch erforderlich ist. Feste Löschungsfristen für die Mitteilungen würden ein umfangreiches – nicht automatisiertes – Wiedervorlagesystem voraussetzen, das die Kammer nachvollziehbar als unverhältnismäßig im Sinne des § 8 Abs. 1 HmbDSG ansieht.

In einem anderen Fall haben wir einen Rechtsanwalt beraten, der sich über eine zeitweise fehlende und eine offensichtlich versehentliche Eintragung im elektronischen Anwaltsregister der Rechtsanwaltskammer beschwert hatte. Angesichts der zwischenzeitlich erfolgten Korrektur der Eintragungen haben wir mangels Erforderlichkeit auf eine Kontaktaufnahme mit der Kammer und auf die Offenbarung des Beschwerdeführers verzichtet.

Die Rechtsanwaltskammer vertritt ihrerseits eine andere Rechtsauffassung: Beschwert sich ein Rechtsanwalt bei der Kammer über ein anderes Mitglied, dürfe und müsse die Kammer dem Beschwerdegegner in jedem Falle von sich aus über den Inhalt der Beschwerde und den Namen des Beschwerdeführers Kenntnis geben. Dies gelte auch dann, wenn die Kammer die Beschwerde bereits selbst und ohne Kontaktaufnahme mit dem Beschwerdegegner als „abwegig“ zurückgewiesen hatte. Die dafür zunächst gegebenen Begründungen konnten uns nicht überzeugen: Weder das allgemeine Recht des Beschwerdegegners auf informationelle Selbstbestimmung, noch die allgemeine Belehrungspflicht der Rechtsanwaltskammer nach § 73 Abs.2 Nr.1 BRAO, noch die Gewährung rechtlichen Gehörs nach § 74 Abs.3 BRAO geben eine notwendige spezialgesetzliche Übermittlungsbefugnis im Sinne des Hamburgischen Datenschutzgesetzes.

Eine nachgereichte Begründung hat uns dann aber doch bewogen, die Erörterungen mit der Kammer nicht fortzuführen, sondern den Beschwerdeführer auf seine eigenen Rechte zu verweisen: Nach Auffassung der Kammer muss der Beschwerdegegner die Möglichkeit einer Selbstanzeige nach § 123 BRAO zur Aufklärung des Verdachts und damit zur „Selbstreinigung“ erhalten. Es ist grundsätzlich anzuerkennen, dass es nicht zwingend zu einer Befriedung führt, wenn die Kammer die Beschwerde eines Mitglieds gegen ein anderes als „abwegig“ zurückweist. Der Beschwerdeführer kann die Kritik auch weiterhin gegenüber seinen Kolleginnen und Kollegen äußern, ohne dass der Kritisierte davon erfährt und sich wehren kann. Obgleich auch § 123 BRAO keine spezialgesetzliche Datenübermittlungsbefugnis gibt, ist diese Argumentation dennoch nachvollziehbar und ihre Umsetzung der Selbstverwaltung der Rechtsanwaltschaft zu überlassen.

Ein anderes Kammermitglied hat sich darüber beschwert, dass die Rechtsanwaltskammer Beitragsrechnungen und Mahnungen ohne einen Vermerk „persönlich / vertraulich“ an die Kanzleiadresse verschickte, sodass die Mitarbeiterinnen und Mitarbeiter hiervon Kenntnis erhielten. Mit der Kammer haben wir hier eine Unterscheidung zwischen Rechnung und Mahnung vereinbart: Während die Kanzleimitarbeiter wissen, dass ein Rechtsanwalt Kammerbeiträge zu zahlen hat, und eine entsprechende Rechnung „neutral“ ist, ist eine Mahnung zugleich mit dem Vorwurf des

Verzugs und damit eines Fehlverhaltens „des Chefs“ verbunden. Dieser Vorwurf sollte nur an den betroffenen Rechtsanwalt persönlich gerichtet werden. Die Rechtsanwaltskammer versendet Mahnungen deswegen nun „persönlich / vertraulich“, Beitragsrechnungen dagegen – auch auf Wunsch vieler Kammermitglieder – nach wie vor ohne diesen Zusatz an die Kanzlei.

6. Strafvollzug

6.1 Beschwerden von Gefangenen

Beschwerden von Gefangenen über angebliche Datenschutzverstöße führten in einem Fall zu einer Bestätigung des behaupteten Sachverhalts. Für die Mitteilung von Entlassungsadressen an Dritte gibt es ein datenschutzgerechtes Verfahren.

Im Berichtszeitraum haben uns 15 Beschwerden von Strafgefangenen erreicht – unter anderem zum Umgang mit Gesundheitsdaten, zur Versagung einer Akteneinsicht, zu Beschränkungen des Telefonkontakts und mehrfach zu unzulässigen Briefkontrollen.

Entweder konnten wir die Eingaben bereits durch eine Erläuterung der Rechtslage nach dem Strafvollzugsgesetz abschließend beantworten, oder wir haben das Strafvollzugsamt um Stellungnahme bzw. weitere Ermittlungen in den Justizvollzugsanstalten (JVA) gebeten. Nur in einem Fall (Offenbarung der Häftlingsnamen an den Zellentüren beim sog. „Angehörigen-Tag“) wurde die Beschwerde bestätigt und für die Zukunft Abhilfe zugesagt.

In anderen Fällen gab die Darstellung des Strafvollzugsamts von Vollzugsregelungen und JVA-Praxis keinen Anlass zu datenschutzrechtlichen Beanstandungen. Aber auch behauptete Datenschutzverstöße, die vom Gefangenen sehr konkret und detailliert geschildert worden waren, sind von den beschuldigten JVA-Bediensteten auf Nachfrage bestritten worden. Für uns besteht in diesen Fällen keine weitere Handlungsmöglichkeit. Ein Gefangener berichtete davon, dass JVA-Bedienstete, über die sich ein Gefangener beschwerte, ihrerseits Disziplinarmaßnahmen gegen den Gefangenen wegen Rufschädigung anstrengen.

Ein Strafgefangener hat sich bei uns darüber beschwert, dass seine Entlassungsadresse auch dann an anfragende Inkassobüros weitergegeben werde, wenn im Melderegister eine Auskunftssperre eingerichtet sei. Unsere Rechtsprüfung und Nachfrage beim Strafvollzugsamt haben Folgendes ergeben: Nach § 120 Abs.5 Hamburgisches Strafvollzugsgesetz (StrVzG) darf die Justizvollzugsanstalt (JVA) die Entlassungsadresse auch

nicht-öffentlichen Stellen wie Gläubigern und Inkassobüros mitteilen, wenn von diesen „ein berechtigtes Interesse an dieser Mitteilung glaubhaft dargelegt wird und die Gefangenen kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben." Deswegen verlangt die JVA von Inkassobüros eine Vollmacht oder eine Abtretungserklärung und hört die Gefangenen in der Regel zu dem Auskunftsersuchen an. Soweit der JVA eine Auskunftssperre zu der Entlassungsadresse nicht bereits bekannt ist, hat der Gefangene hier die Gelegenheit, auf sie hinzuweisen. Liegen keine entsprechenden Beschlüsse eines Gerichts oder der Staatsanwaltschaft vor, ist der Gefangene aber nicht verpflichtet, überhaupt eine Entlassungsadresse zu benennen.

Wurde der Strafgefangene schon vor der Adressanfrage entlassen, informiert die JVA den Entlassenen schriftlich über die Anfrage – soweit ihr die Adresse bekannt ist – und gibt ihm Gelegenheit, innerhalb von 2 Wochen mögliche schutzwürdige Interessen zu benennen. Nimmt der Entlassene diese Möglichkeit nicht wahr oder kommt der Brief mit „unbekannt verzogen" zurück, teilt die JVA dem Dritten bei Darlegung des berechtigten Interesses die – ggf. nicht mehr aktuelle – Adresse mit. In diesen Fällen wird nach § 120 Abs.5 Satz 4 StrVzG die Auskunft auch ohne vorherige Anhörung erteilt, weil sonst der „Zweck der Mitteilung vereitelt" würde. Auch eine nicht mehr zutreffende Adresse ist z. B. für ein Inkassounternehmen durchaus von Wert. Wir haben gegen dieses Verfahren keine Bedenken geltend gemacht und den Gefangenen entsprechend beschieden.

6.2 Einsicht in Gefangenenakten durch den Anti-Folter-Ausschuss des Europarats

Mit einem Kompromiss ließe sich sowohl dem deutschen Einwilligungsvorbehalt als auch dem Wunsch des Anti-Folter-Ausschusses nach unbeschränktem Zugang zu den Akten Rechnung tragen.

Von besonderer datenschutzrechtlicher Bedeutung war eine Anfrage des Strafvollzugsamtes, ob die Justizvollzugsanstalten (JVA) dem Europäischen Ausschuss zur Verhütung von Folter (CPT) die Gefangenenakten zur Verfügung stellen dürfen bzw. müssen. Der CPT hatte sich beim zuständigen Bundesministerium darüber beschwert, dass in Deutschland der Zugang zu Gefangenenunterlagen an die individuelle Einwilligung der Betroffenen geknüpft und damit regelmäßig stark verzögert werde.

In § 30 Abs.3 und indirekt in § 32 Abs.1 Hamburgisches Strafvollzugsgesetz (StrVzG) wird dem Gefangenen die überwachungsfreie Kommunikation mit dem CPT garantiert. Die Datenverarbeitungsvorschriften der §§ 120 ff StrVzG geben den JVA aber keine Befugnis zur Weitergabe von

Gefangenenakten an den CPT. Es bedarf deswegen tatsächlich der Einholung einer Einwilligung. Dies sollte jedoch weitestgehend unabhängig von der Anstaltsleitung oder anderen Strafvollstreckungsbehörden erfolgen.

Wir haben der Justizbehörde einen Kompromiss vorgeschlagen, der insbesondere berücksichtigt, dass der CPT gerade dafür da ist, Gefangene zu schützen und ihre Interessen zu wahren, ohne dabei von staatlichen Stellen beschränkt zu werden: Die JVA könnte in einem Aushang und durch direkte mündliche Kommunikation den Besuch des CPT ankündigen und dessen Kontaktdaten nennen. Das würde es den Gefangenen, die sich an den CPT wenden möchten, ermöglichen, von sich aus – und nicht überwacht – schriftlich oder telefonisch oder beim Besuch den oder die Vertreter des CPT anzusprechen.

Wir haben es aber auch für datenschutzrechtlich vertretbar gehalten, sich im vorliegenden Fall ausnahmsweise – wegen der besonderen Aufgabe des CPT – mit einer konkludenten Einwilligung zu begnügen. § 5 Abs.2 Satz 1 HmbDSG ermöglicht eine Einwilligung in anderer als schriftlicher Form, wenn „besondere Umstände“ dies angemessen erscheinen lassen. Danach könnte die Anstaltsleitung den Besuch des CPT in der Anstalt ankündigen und dabei auf Folgendes hinweisen: Die Anstaltsleitung gehe davon aus, dass die Gefangenen mit der Akteneinsicht durch die Vertreter des CPT einverstanden sind – es sei denn, ein Gefangener widerspricht dem ausdrücklich. Im „beredten“ Schweigen läge dann die konkludente Einwilligung. Entscheidend ist allerdings, dass wirklich jeder Gefangene die Bekanntmachung und Vermutung der Einwilligung rechtzeitig vor dem Besuch des CPT zur Kenntnis nimmt. Sonst kann das Schweigen nicht als konkludente Willensäußerung gewertet werden.

7. Soziales

7.1 Großprojekt Jugend, Soziales und Wohnen: noch rechtliche Fragen offen

Weiterhin ist eine Klärung erforderlich, auf welcher Rechtsgrundlage das Verfahren in Betrieb genommen werden soll. In diesem Rahmen muss das IT-Verfahren dann einer abschließenden Prüfung aller einschlägigen Vorschriften unterzogen werden, bevor es in Betrieb genommen wird.

Das Projekt JUS-IT hat den Auftrag, die Entwicklung einer weitgehend integrierten Softwarelösung für die Bereiche Jugend, Soziales und Wohnen unter der Berücksichtigung der Organisation der Sozialen Dienstleistungszentren fachlich, organisatorisch und unter Absicherung der erforderlichen Ressourcen umzusetzen. Mit Hilfe der neuen IT-Lösung soll ein integrier-

tes Eingangs- und Fallmanagement für diese Aufgabenfelder unterstützt und die Geschäftsprozesse aus einem Guss bearbeitet werden. Damit werden u. a. die Ziele verfolgt, die kundenzentrierte Hilfestellung zu verbessern, die Bearbeitung zu vereinfachen und durch eine Entlastung von Verwaltungstätigkeiten die kundenbezogene Betreuungskapazität zu erhöhen. Mit dem neuen Verfahren sollen die bisher genutzten, getrennten IT-Verfahren PROJUGA, PROSA und DIWOGE abgelöst werden.

Wie schon bei dem Vorprojekt und in der Ausschreibungsphase wurden wir seit Beginn des Projekts JUS-IT intensiv eingebunden und haben so frühzeitig die Chance wahrgenommen, die datenschutzrechtlichen Anforderungen in die Projektarbeit einzubringen und das Projekt bei der Erstellung des Datenschutzkonzeptes zu beraten.

Wir haben von Beginn an darauf hingewiesen, dass die Nutzung einer gemeinsamen Datenbasis für die unterschiedlichen Aufgabenbereiche rechtlich nur zulässig ist, wenn die Voraussetzungen, die hierfür im Sozialgesetzbuch festgeschrieben sind, eingehalten werden. Hierbei sind insbesondere die §§ 67c, 67d, 69 und 79 SGB X zu beachten. Eine abschließende Darlegung, aus der die Einhaltung dieser Voraussetzungen nachvollziehbar ist, enthält der derzeitige Entwurf des Datenschutzkonzeptes jedoch noch nicht.

Auch die Frage, ob eine gemeinsame Stammdatenverarbeitung für unterschiedliche Rechtsgebiete zulässig ist, muss in diesem Zusammenhang vom Projekt noch aufgearbeitet und abschließend geklärt werden. Rechtlich würde nämlich bereits dann eine Datenübermittlung vorliegen, wenn ein Klient mit einem Anliegen auf die Behörde zukommt und dabei festgestellt werden kann, dass seine Stammdaten bereits vorliegen, weil er bereits mit einem Anliegen aus einem anderen der Rechtsgebiete, in denen JUS-IT eingesetzt wird, in Berührung gekommen ist. Eine solche Übermittlung ist insbesondere nur zulässig, sofern die Voraussetzungen nach § 67d und § 69 SGB X vorliegen. Im Wesentlichen bedeutet dies, dass sowohl die Erforderlichkeit für eine gemeinsame Stammdatenverwaltung gegeben als auch die Verhältnismäßigkeit einer solchen Verarbeitung gewahrt ist. Dabei ist eine solche gemeinsame Datenverarbeitung nur denkbar für Sozialleistungsträger, wie sie in § 12 SGB I in Verbindung mit §§ 18 bis 29 SGB I definiert sind. Unter Einhaltung restriktiver Zugriffsberechtigungen und mit einem jeweils auf die spezifische Situation zugeschnittenen Profil an einzusehenden Daten kann dies nach unserer derzeitiger Auffassung grundsätzlich zulässig sein, ohne das Sozialgeheimnis nach § 35 SGB I zu gefährden.

Eine gemeinsame Datenverarbeitung mit anderen Stellen, etwa behördlichen Stellen, die nicht zu den Sozialleistungsträgern gehören, oder freien Trägern oder ein automatisierter Abruf von Daten durch solche Stellen ist von den Regelungen des SGB jedoch in keinem Fall gedeckt.

Da die im Raum stehende Rechtsfrage für die weitere Entwicklung von JUS-IT von grundsätzlicher Bedeutung für die gesamte IT-Lösung ist, haben wir wiederholt auf diesen nach wie vor offenen Punkt hingewiesen und auch den Vorschlag unterbreitet, in einem parallelen Projekt den Schwerpunkt auf dem Aspekt der Organisationsentwicklung zu legen. Das Ziel des Senats, durch Integration der verschiedenen Perspektiven, z. B. der Jugend- und der Sozialhilfe, die Hilfe wirksamer zu gestalten, könnte so rechtssicher erreicht werden.

Ab August 2010 haben wir darüber hinaus zu zahlreichen Feinspezifikationen (u. a. Schnittstelle zu Polizei-Verfahren; Löschen, Massendruck, Protokollierung) eine Stellungnahme abgegeben und sind mit dem Projekt in regelmäßigen Gesprächen, um eine datenschutzgerechte Lösung für die zahlreichen Detailfragen zu finden. Zu den Hinweisen, die wir gegeben haben und die zu beachten sind, gehören beispielsweise,

- dass zum Teil zu lange Löschungsfristen festgelegt wurden, die sich aus den fachlichen Anforderungen nicht ergeben,
- dass bei einem Fremdzugriff auf einzelne Vorgänge in jedem Fall der zuständige Sachbearbeiter zeitnah automatisiert über die Tatsache des Zugriffs zu informieren ist,
- dass im Rahmen des Projekts eine sichere Authentisierung z. B. unter Nutzung einer Chipkarte umgesetzt werden sollte,
- dass die Rechtsgrundlage einer elektronischen Aktenführung geklärt und die Anforderungen an elektronische Akten noch spezifiziert werden müssen und
- dass bei der Bildung von Aktenzeichen darauf verzichtet werden sollte, dass darin personenbezogene Inhalte wie z. B. Geburtsdatum und Namensbestandteile enthalten sind.

Die Entwicklung des Projektes JUS-IT werden wir weiter begleiten.

7.2 Gemeinsame Fallkonferenzen über junge Gewalttäter

Die Umsetzung der neuen Fallkonferenzen offenbart datenschutzrechtliche Mängel.

Über die bisherige Praxis der behördenübergreifenden Fallkonferenzen haben wir in der Vergangenheit ausführlich berichtet (vgl. 22. TB, 7.6). Dabei haben wir neben einigen Einzelpunkten im Wesentlichen kritisiert,

dass die koordinierende Stelle für diese Fallkonferenzen nicht beim Jugendamt, sondern bei der Polizei angesiedelt ist. So fließen bei der Polizei die meisten Erkenntnisse zusammen, obwohl beispielsweise die Jugendämter einen weitaus geringeren Spielraum zur Datenübermittlung an die Polizei haben als umgekehrt die Polizei an die Jugendämter. Zudem ist das Jugendamt die sachnächste Stelle für Jugendhilfeangelegenheiten.

Im Jahr 2011 hat der Senat entschieden, das bisherige Modell zu modifizieren. Die Fallkonferenzen sollen in Zukunft erheblich ausgeweitet werden und an feststehenden Terminen stattfinden. Grundlage für die Einberufung einer Fallkonferenz soll zukünftig ein Ampelmodell sein. Darin zeigen die einzelnen Behörden bei Jugendlichen und jungen Erwachsenen über die Signalfarben grün, gelb und rot an, ob eine (ggf. weitere) Fallkonferenz erforderlich ist. Hierfür sind für die einzelnen Behörden gesonderte Eingabetabellen angelegt worden, die ausschließlich die jeweilige Behörde verändern können und auf die nur die Koordinierungsstelle einen lesenden Zugriff hat. Die farbliche Einstufung wird mit einem kurzen Hinweis hinterlegt. Die Meldung gelb bedeutet eine Obachtphase. Die Stufe rot intendiert die kurzfristige Einberufung einer Fallkonferenz. Eine Schaltung der Ampel führt jedoch nicht zu einer automatischen Einberufung einer Fallkonferenz. Vielmehr erfolgt eine Einzelfallentscheidung durch den Koordinator unter Berücksichtigung weiterer Kriterien und der von den anderen Stellen mitgeteilten Informationen. Die Koordinatorenfunktion übernimmt weiterhin die Polizei in Form des Präsidialstabes 3 „Fachdienststelle zur Bekämpfung der Jugendkriminalität“.

Im Gegensatz zum bisherigen Modell soll es dadurch möglich sein, dass eine Fallkonferenz einberufen wird, obwohl sämtliche beteiligte Stellen aufgrund der bei ihnen vorhandenen Informationen eine solche noch nicht für zwingend erforderlich halten. Denn erst die Gesamtschau der mitgeteilten Ergebnisse soll eine hinreichende Entscheidungsgrundlage dafür sein, ob die Einberufung einer Fallkonferenz aus Sicht der Polizei geboten erscheint.

Die Polizei als Koordinator hat zu gewährleisten, dass die von den beteiligten Behörden verwalteten und bei ihnen zusammengeführten Informationen von ihr ausschließlich für die Entscheidung der Einberufung einer Fallkonferenz (ja/nein) und den daraus folgenden Maßnahmen verwandt werden. Die Informationen sollen insbesondere in technischer, organisatorischer und personeller Hinsicht von der sonstigen Sachbearbeitung der Polizei getrennt sein. Sie sollen wie bisher erst an die eigene und an die übrigen im jeweiligen Einzelfall zuständigen Behörden weitergegeben werden, wenn eine Fallkonferenz einberufen wird. Die Löschung der Informationen soll durch den Koordinator veranlasst werden, wenn der Betroffene

nicht mehr die Voraussetzungen für eine Einstufung als Kandidat der Fallkonferenz erfüllt. Dies ist zumindest dann der Fall, wenn er das 21. Lebensjahr vollendet hat. Die übrigen Behörden können eine vorherige Löschung anregen.

Die Zusammenarbeit der Behörden soll technisch über einen Sharepoint erfolgen. Auf der Grundlage des jeweils für sie geltenden Datenschutzrechts sollen sie mit Hilfe des Sharepoints die Informationen an die Koordinierungsstelle weitergeben.

An der Entwicklung des Ampelmodells sind wir auf Referentenebene beteiligt worden. Wir hatten somit Gelegenheit zur Beratung und konnten dabei einige datenschutzrechtliche Hinweise geben. Dies betraf beispielsweise die Ausgestaltung der Personalbögen, das Löschkonzept und die Übermittlungsbefugnisse einschließlich etwaiger Einwilligungserklärungen. Allerdings sind wir an der technischen Realisierung des Sharepoints nicht beteiligt worden, obwohl wir ausdrücklich darum gebeten hatten. Erst durch Medienberichte haben wir davon erfahren, dass das neue Verfahren bei Fallkonferenzen in Produktion gegangen ist, ohne dies abschließend mit uns abzustimmen. Aus diesem Anlass haben wir das IT-Verfahren im Rahmen unserer Überwachungsbefugnisse nach § 23 HmbDSG einer Prüfung unterzogen. Dabei zeigten sich einige technische – aber auch rechtliche –Schwachstellen, die uns dazu veranlasst haben, Forderungen nach einer Verbesserung des Datenschutzes zu erheben.

Es fehlte nicht nur eine Risikoanalyse und eine Verfahrensbeschreibung, sondern die Polizei hätte als verantwortliche Stelle auch eine Errichtungsanordnung erstellen müssen. Ferner sah das Verfahren vor, dass an die Staatsanwaltschaft auch die Daten der Personen unter 14 Jahren übermittelt werden, obwohl für diesen Personenkreis die Staatsanwaltschaft keine Zuständigkeit hat. Kritisiert worden war von uns auch, dass sämtliche Ampelschaltungen für alle beteiligten Stellen jederzeit sichtbar sind, unabhängig davon, ob eine Fallkonferenz bevorsteht und unabhängig davon, ob eine Kenntnis von der Bewertung durch andere Stellen im Einzelfall erforderlich ist. Das produktiv genutzte Verfahren wurde daraufhin kurzfristig in der Nutzung eingeschränkt, und die Daten verarbeitende Stelle hat angekündigt, unsere Forderungen in einem fortgeschriebenen IT-Verfahren umzusetzen.

Darüber hinaus ist die Anbindung der Koordinierungsstelle an die Polizei mit den sich daraus ergebenden Folgeproblemen ein Kernkritikpunkt.

Wir haben unsere Auffassung wiederholt, dass eine Anbindung der Koordinierungsstelle bei der Polizei zu erheblichen datenschutzrechtlichen Problemen führt. Eine Anbindung der Koordinierungsstelle als Empfängerin

der verschiedenen Datenübermittlungen bei der Behörde für Arbeit, Soziales, Familie und Integration (BASFI) ist unseres Erachtens sachnäher, da Kern des Konzepts nicht in erster Linie die Gefahrenabwehr, sondern die Jugendhilfe, also die Verhütung von Kindes- und Jungendwohlgefährdungen ist. Problematisch ist u. a., dass die Polizeibeamten dem Legalitätsprinzip unterliegen, was im Einzelfall zu Widersprüchen zu dem am Wohl des Kindes, des Jugendlichen oder Heranwachsenden orientierten Verfahrenszweck führen kann. Da die Dienststellen der BASFI bei der Erhebung von Daten die weitreichendsten und bei der Datenübermittlung eher restriktive Befugnisnormen zu berücksichtigen haben, ist die Gefahr rechtswidriger Datenübermittlungen erheblich höher, wenn die Polizei als Koordinierungsstelle fungiert. Besonders problematisch ist in diesem Zusammenhang, dass es der Polizei möglicherweise an einer hinreichenden Befugnis zur Datenerhebung fehlt. Eine solche kann sich zwar aus § 6 Nr. 6 PolDVG ergeben. Dessen Voraussetzungen sind allerdings so eng, dass es fraglich ist, ob diese für alle für das Ampelverfahren vorgesehenen Fälle vorliegen. Dies ist nach dem Gesetzeswortlaut nur dann der Fall, „wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person künftig Straftaten begehen wird, und die Erhebung zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung erforderlich ist“.

Die Projektgruppe hat unsere Kritik zwar konstruktiv aufgenommen, dennoch wurde letztlich entschieden, dass es bei der Anbindung der Koordinierungsstelle bei der Polizei bleiben soll. Kurz vor Redaktionsschluss erreichten uns noch die bislang fehlenden rechtlichen und technischen Unterlagen zum IT-Verfahren (Errichtungsanordnung, Risikoanalyse, Übersicht über die Datenverarbeitungsbefugnisse der beteiligten Stellen). Wir haben bereits angekündigt, dass wir auch aufgrund des engen Befugniskorridors, welcher der Polizei als datenverarbeitender Stelle eröffnet ist, die Einhaltung der datenschutzrechtlichen Vorgaben kontrollieren werden. Zudem ist durch einen Protokollmechanismus sicherzustellen, dass fehlerhafte und unzulässige Zugriffe erkannt werden.

Es sind kaum sensiblere Informationen über junge Menschen denkbar, als deren Kategorisierung als Intensivtäter. Es ist daher erforderlich, auch künftig das Ampelkonzept und seine Umsetzung datenschutzrechtlich kritisch zu begleiten. Wir werden deshalb im nächsten Tätigkeitsbericht wieder darauf zurückkommen.

7.3 Leistungen für Bildung und Teilhabe (Bildungspaket)

Nach anfänglichen Schwierigkeiten ist es gelungen, in Hamburg die Umsetzung des Bildungspakets datenschutzgerecht zu gestalten.

Das Gesetz zur Ermittlung von Regelbedarfen und zur Änderung des Zweiten und des Zwölften Sozialgesetzbuches ist am 29. März 2011 im Bundesgesetzblatt veröffentlicht worden und rückwirkend zum 1. Januar 2011 in Kraft getreten. Neben weiteren sozialrechtlichen Regelungen enthält das Gesetz vor allem Regelungen zu Leistungen für Bildung und Teilhabe für Kinder, Jugendliche und junge Erwachsene – das sogenannte Bildungspaket. Wir haben das Verfahren zur Umsetzung dieses Angebots in Hamburg datenschutzrechtlich begleitet.

Das Hamburger Modell sieht ein Verfahren vor, das auf ein Minimum an Verwaltungsaufwand und damit verbundene Kosten ausgerichtet ist. Gutscheine werden in Hamburg nicht benötigt. Die Behörde für Arbeit, Soziales, Familie und Integration (BASFI) erstellt eine Liste mit Anbietern, die bereit und geeignet sind, Leistungen für Bildung und Teilhabe zu erbringen. Diese Liste ist offen und soll über die Zeit wachsen. Potentielle Anbieter werden ausdrücklich aufgefordert, an dem Verfahren teilzunehmen und sich registrieren zu lassen.

Um eine einmalige oder fortlaufende Leistung zu erhalten, kann der Leistungsberechtigte wählen, ob er bei dem teilnehmenden Leistungsanbieter entweder seinen Bewilligungsbescheid oder eine gesonderte Bescheinigung (Leistungsbestätigung) vorlegen will. Diese Wahlmöglichkeit wurde erst auf Grund unserer Intervention eingeführt, denn mit der Vorlage des gesamten Leistungsbescheids werden sensible persönliche Daten bei Trägern und Vereinen offengelegt, die für das Bildungspaket überhaupt nicht benötigt werden.

Bezieher von Leistungen nach dem SGB XII, § 2 Asylbewerberleistungsgesetz (AsylbLG) oder von Wohngeld oder Kinderzuschlag erhalten automatisch eine solche gesonderte Bescheinigung, aus der sich lediglich die für die Leistungsanbieter relevanten Daten ergeben. Dabei handelt es sich um folgende Angaben des Berechtigten:

- Name, Vorname,
- Geburtsdatum,
- Adresse,
- Bescheid vom,
- Bewilligungszeitraum,
- Art der Leistung.

Beziehern von Leistungen nach dem SGB II kann eine solche Bescheinigung wegen der Besonderheiten des in den Jobcentern eingesetzten EDV-Verfahrens bislang nicht im automatisierten Verfahren übersandt werden. Dieser Personenkreis kann aber ebenfalls eine solche Bescheinigung

erhalten, wenn er nur die für die Leistung wesentlichen Daten und nicht die im Bewilligungsbescheid zusätzlich enthaltenen Angaben offenlegen will. Die Bescheinigung muss dann aber im Einzelfall beim zuständigen Jobcenter beantragt werden.

Die Leistungsanbieter sind von der BASFI schriftlich darauf hingewiesen worden, dass sie aus datenschutzrechtlichen Gründen den Bewilligungsbescheid nicht kopieren dürfen. Jede Verwendung (Verarbeitung und Nutzung) der übermittelten Daten, die von dem Übermittlungszweck nicht gedeckt sind, ist zu unterlassen. Die übermittelten Sozialdaten sind geheim zu halten und ihre Mitarbeiter sind entsprechend zu verpflichten. Die Daten sind von den Leistungsanbietern zu löschen, sobald die Behörde ihnen den ihnen zustehenden Betrag überwiesen hat.

Es ist sichergestellt, dass die Leistungsberechtigten über das Verfahren – und insbesondere über die Wahlmöglichkeit des Nachweises der Leistungsberechtigung – in Kenntnis gesetzt werden. Dies gilt auch für die nach dem SGB II Leistungsberechtigten. Im Ergebnis ist dies somit ein gutes Beispiel dafür, wie durch unsere rechtzeitige Beteiligung ein insgesamt gesetzeskonformes Verfahren entwickelt werden kann.

8. Bildung

8.1 Initiative „Meine Daten kriegt ihr nicht!“

Die Datenschutzkompetenzförderung an Schulen bewegt sich nur in ganz kleinen Schritten nach vorn.

Im Berichtszeitraum wurde die Pilotphase der Initiative, die von uns im Jahr 2009 angestoßen worden ist (vgl. 22. TB, 3.1.2) beendet. Ausgangspunkt des Projekts war die Erkenntnis, dass das Leben in der digitalen Gesellschaft erlernt und eingeübt werden muss und dass den Schulen eine zentrale Funktion für die Datenschutzkompetenzförderung junger Menschen zukommt. Klar ist auch, dass die digitale Gesellschaft keine Schonzeit kennt: Das Eintrittsalter in die sozialen Netzwerke liegt noch unterhalb der persönlichen Schuldfähigkeit im Strafrecht. Die Angebote, die Kinder im Netz erwarten, beginnen nicht selten schon im Grundschulalter. Gerade auch für den schulischen Alltag nutzen Schüler das Internet als Nachschlags- und Wissensquelle. Es besteht dringender Handlungsbedarf.

Es ist daher wichtig, dass die Initiative auf dem eingeschlagenen Weg zügig weiter voranschreitet. Nun gilt es, der Initiative ein breiteres Anwendungsfeld vor Ort zu sichern. Der Schlüssel zum Ziel, alle Hamburger Schulen mit dem Bildungsangebot zu erreichen, führt nur über die Weitergabe der Qualifikationen und Kompetenzen zur Informationsvermittlung an

diejenigen, die für eine Transformation des Wissens vor Ort von Berufs wegen eintreten: Gemeint sind alle Lehrkräfte an Hamburgs Schulen.

Um dieses Ziel zu erreichen, wurde auf unsere Anregung hin eine Handreichung für Lehrerinnen und Lehrer von einem Lehrer der Stadtteilschule Walddörfer erstellt. Neben dem Landesinstitut für Lehrerbildung und Schulentwicklung (LI) und dem Lehrstuhl für Erziehungswissenschaft der Universität Hamburg haben wir beratend an der Erstellung der Handreichung mitgewirkt. Sie soll es den Lehrkräften künftig erleichtern, eigenständig einen Unterricht zur Förderung der Datenschutzkompetenz an ihren Schulen zu entwickeln und vor Ort anzubieten. Die Handreichung wurde im Rahmen eines Projekts an der Kooperativen Schule Tonndorf im Januar 2011 der Öffentlichkeit vorgestellt.

Leider ist diese Handreichung, die konkret einen Vorschlag für eine Unterrichtseinheit beinhaltet, bislang nur sehr zögerlich von den Schulen abgerufen und eingesetzt worden. Die Fortbildungsveranstaltungen, die sowohl das LI als auch wir den Schulen insgesamt, aber auch ausgewählten Lehrkräften anbieten, reichen nicht aus, um eine nachhaltige Verankerung des Projekts zu ermöglichen.

Ziel muss es vielmehr sein, so rasch wie möglich die Datenschutzkompetenzförderung verbindlich als Unterrichtsziel festzuschreiben. Am ehesten wird man dies erreichen können, wenn entsprechende Festlegungen in den für die Schulen verbindlichen Rahmenplänen getroffen werden. Wir werden unser Angebot, vor Ort Schulungen durchzuführen, weiter aufrecht erhalten. Parallel dazu werden wir weitere Anstrengungen unternehmen, um die Initiative nachhaltig zu gestalten.

8.2 Neue Schul-Datenschutzverordnung

Die neue Verordnung schafft in weiten Teilen die erforderliche Klarheit. Dennoch gibt es weiterhin einen zentralen Kritikpunkt.

Die bisher geltende Fassung der Schul-Datenschutzverordnung (Schul-DSVO) bedurfte einer umfangreichen Ergänzung, um die im Oktober 2009 in Form des § 31 Abs. 4 Hamburgisches Schulgesetz (HmbSG) in Kraft getretene Rechtsgrundlage zur Videoüberwachung in Schulen umzusetzen (vgl. 22. TB, 8.1). Zudem wurden einzelne schwer auffindbare Bestimmungen und Richtlinien zum Datenschutz im Schulrecht in die Verordnung integriert, um für mehr Einheitlichkeit und Übersicht zu sorgen. Hierbei geht es insbesondere um die Anlage und das Führen von Schülerbögen (das sind die Schülerakten) und sonstigen Schülerpapieren. Die hiermit verbundenen Klarstellungen sind wichtig und werden von uns begrüßt.

Kritisiert haben wir die Regelung des § 6 Schul-DSVO zur Schulstatistik, denn sie steht nicht im Einklang mit § 8 Abs. 4 Hamburgisches Statistikgesetz (HmbStatG). Zwar dürfen nach dem Statistikgesetz die im Geschäftsgang der Schulen rechtmäßig anfallenden Daten der zuständigen Fachbehörde – das ist die Behörde für Schule und Berufsbildung (BSB) – übermittelt werden. Vor der Übermittlung sind die Daten aber zu anonymisieren, sodass ein Personenbezug nicht erkennbar ist. Nach der Gesetzesbegründung zum Statistikgesetz (Bürgerschaftsdrucksache 13/6831) heißt dies, dass zum Schutz der Persönlichkeitsrechte der Betroffenen die Daten vor ihrer Übermittlung zu anonymisieren sind, so dass die Fachbehörde nicht auf eine Person rückschließen kann.

§ 6 Abs. 1 Schul-DSVO erlaubt es dagegen nicht nur den Schulen, sondern auch der BSB, eine Reihe von personenbezogenen Daten im Rahmen der Schulstatistik zu verarbeiten. Dies kann sich aber nur auf Daten beziehen, die von den Schulen und der BSB im Rahmen ihrer jeweiligen Aufgabenerfüllung zulässigerweise erhoben worden sind. Eine Befugnis zur Weiterleitung personenbezogener Daten durch die Schulen an die BSB zum Zwecke der Statistik kann daraus nicht hergeleitet werden. Vielmehr haben die Schulen wegen des eindeutigen Wortlauts von § 8 Abs. 4 Satz 2 HmbStatG die Daten, die nach § 6 Abs. 1 Schul-DSVO an die BSB weitergeleitet werden sollen, vorher zu anonymisieren. Hierzu bedarf es einer entsprechenden Klarstellung in § 6 Abs. 1 Schul-DSVO, zu der sich die BSB aber nicht durchringen konnte.

Zur Begründung hat die BSB auf § 98 Abs. 2 HmbSG verwiesen. Danach ist bei der Verarbeitung personenbezogener Daten zum Zwecke der Schulstatistik sicherzustellen, dass der Personenbezug außerhalb der staatlichen Schulen und der zuständigen Behörde nicht mehr herzustellen ist. Dieser Hinweis geht aber aus unserer Sicht leer, denn der Regelungsgehalt dieser Vorschrift ist nicht identisch mit der des § 8 Abs. 4 HmbStatG. Vielmehr handelt es sich dabei um eine Aufgabenzuweisungsnorm, ohne dass damit den Schulen die Befugnis erteilt wird, Daten in personenbezogener Form für statistische Zwecke an die BSB zu übermitteln.

Einzuräumen ist, dass es diesen Mangel bereits in der bisherigen Fassung der Schul-DSVO gab. Wir haben aber die Problematik bereits vor Einführung der alten Schul-DSVO im Jahre 2006 thematisiert, ohne dass sich seinerzeit der Verordnungsgeber unserer Kritik angeschlossen hat. Wegen der unverändert bestehenden Rechtslage mussten wir anlässlich der Novellierung der Schul-DSVO erneut auf diesen Mangel hinweisen. Leider auch diesmal ohne Erfolg.

Die BSB hat sich aber auf unser Drängen bereit erklärt, zu der Problematik ein Rechtsgutachten einzuholen. Kurz vor Redaktionsschluss erfuhren wir, dass die BSB in konkreten Verhandlungen mit einem externen Gutachter steht. Es bleibt abzuwarten, ob er zur Übernahme des Gutachtens bereit ist und damit der zwischen uns und der BSB bestehende grundsätzliche Dissens aufgelöst werden kann.

8.3 Zentrales Schülerregister

Unsere Prüfung des Verfahrens konnte nicht abgeschlossen werden. Es droht, dass sich daraus eine unendliche Geschichte entwickelt.

Das Zentrale Schülerregister (ZSR) ist von Beginn an auf Bedenken gestoßen (vgl. zuletzt 22. TB, 8.3). Die Prüfung, die wir im letzten Berichtszeitraum begonnen hatten, haben wir in diesem Berichtszeitraum fortgesetzt und insbesondere die technisch-organisatorischen Maßnahmen geprüft, die im Zusammenhang mit dem automatisierten Abruf von Daten aus dem ZSR durch andere Behörden getroffen worden sind. Nach § 10 Schul-Datenschutzverordnung (Schul-DSVO) darf ein solcher Abruf für hamburgische Polizeivollzugsdienststellen, Jugendämter und Gesundheitsämter eingerichtet werden.

Bei unseren Ermittlungen vor Ort mussten wir feststellen, dass die Sachlage entweder mit den Rechtsgrundlagen oder mit den Unterlagen, die wir von der Behörde für Schule und Berufsbildung (BSB) erhalten hatten, nicht übereinstimmte. Diesen Dingen musste bis ins kleinste Detail nachgegangen werden, was den Fortgang der Prüfung nicht beschleunigte. Zur Illustration hier einige Beispiele:

- Nach § 10 Abs. 2 Satz 2 Schul-DSVO sind die Abrufe zur Kontrolle ihrer Zulässigkeit u. a. mit der Kennung des zum Abruf zugelassenen Datenendgerätes und der Dienstnummer des abrufenden Bediensteten zu protokollieren und sechs Monate zu speichern. In dem fachlichen Feinkonzept, das uns vorliegt, ist das Abrufverfahren der Polizei entsprechend beschrieben. Danach soll eine systemseitige Protokollierung aller erfolgten Sucheingaben und -ergebnisse erfolgen, welche für Stichprobenprüfungen abgerufen werden können. Bei der Prüfung dieser Protokolle vor Ort stellten wir jedoch fest, dass im Feld Nutzerkennung und Datenendgerät immer das gleiche Datum ausgewiesen wurde. Anhand der systemseitigen Protokollierung konnte damit nicht nachvollzogen werden, welcher Nutzer von welchem Datenendgerät auf das ZSR zugegriffen hat. Eine regelmäßige Stichprobenkontrolle der

Zulässigkeit der Abrufe erfolgt jedoch regelmäßig auf der Grundlage der systemseitigen sowie einer ergänzenden manuellen Protokollierung.

Wie sich herausstellte, resultierten die Protokolleinträge hauptsächlich aus der Art der technischen Anbindung der Polizei an das ZSR, bei der eine Protokollierung des Datenendgerätes nicht möglich ist. Außerdem stehen dem die organisatorischen Regelungen zur Nutzung entgegen, denn bislang ist allein der Führungslagedienst berechtigt, Daten aus dem ZSR abzurufen. Diese Daten werden dann vom Führungslagedienst den anfragenden Kollegen vor Ort mitgeteilt, damit sie beispielsweise die zuständige Schule für aufgegriffene, vermeintliche Schulschwänzer ermitteln können. Die rechtlich vorgegebenen Protokollierungsdaten (Anfragender, Grund, Zeit etc.) werden ergänzend manuell protokolliert. Die Zugriffe des Führungslagedienstes auf das ZSR erfolgen hierbei unter einer Benutzerkennung, die nicht personengebunden ist. Das dazugehörige Passwort wurde bei Einrichtung durch die BSB vergeben und beibehalten.

Das Verfahren der Polizei entspricht damit in Teilen nicht den rechtlichen Vorgaben und weicht von der Feinkonzeption ab, die uns vorgelegt wurde. Die BSB und die Polizei sind sich dieser Mängel bewusst und haben Abhilfe zugesagt.

- Bei einem Besuch des Gesundheitsamtes Altona stellten wir fest, dass nicht klar war, welche Stelle über bestehende Zugriffsberechtigungen Auskunft geben kann. Im Gesundheitsamt existierte jedenfalls dazu keine Aufstellung, so dass wir an die IuK-Abteilung des Bezirksamtes Altona, an die zentrale Stelle für IT-Angelegenheiten der Bezirksverwaltung und an die BSB verwiesen wurden. Letztendlich konnte die BSB aufklären, dass jedes Bezirksamt entsprechende Berechtigungsgruppen vergibt und die Mitglieder bestimmt.

- Nach § 11 Meldedatenübermittlungsverordnung (MDÜV) werden regelmäßig Meldedaten an das ZSR übermittelt, damit das Register über valide Daten verfügt und ordnungsgemäß geführt werden kann. Zu diesen Daten gehören auch die nach § 34 Abs. 5 Hamburgisches Meldegesetz (HmbMG) eingerichteten Auskunftssperren, die insbesondere dem Zweck dienen, Leib und Leben der Betroffenen zu schützen. Anschriften mit melderechtlicher Auskunftssperre unterliegen deshalb einem hohen Schutzbedarf. Eine Verletzung der Vertraulichkeit dieser Daten kann für den Betroffenen im Einzelfall schwerwiegende Folgen haben. Der Schutz dieser Daten muss daher im gesamten Verarbeitungsprozess gewährleistet werden. Wir haben Zweifel, ob die hierfür erforderlichen Maßnahmen getroffen worden sind.

Unsere Prüfung in einer Schule zeigte zwar, dass der Anwender auf eine bestehende Auskunftssperre hingewiesen wird. Wird ein Fall mit Auskunftssperre aufgerufen, erscheint vor dem Aufruf der Detaildaten ein entsprechender deutlicher Hinweis. Es liegen aber seitens der BSB keine Handlungsanweisungen vor, wie anschließend mit solchen Daten umzugehen ist. Deshalb versuchen die Anwender, dieser Misere mit einer gewissen Kreativität zu begegnen. Beispielsweise werden die Adressdaten in der Schulverwaltungssoftware durch die Adresse der Schule ersetzt, damit nicht versehentlich eine geschützte Adresse offenbart wird. Hierfür bedarf es aber einer einheitlichen Verfahrensweise, die von der BSB vorzugeben ist.

- Die Datenverarbeitung in einer Schule ist nach den Regelungen der Schul-DSVO auf die Personen begrenzt, die diese Schule besuchen, besucht haben, besuchen wollen oder besuchen sollen. Unser Kontrollbesuch in einer Schule zeigte, dass diese Regel sehr weit ausgelegt wird. So war es der Schulsekretärin möglich, unter Angabe des Geburtsdatums sowie des vollständigen Vor- und Familiennamens Kinder zu finden, für die diese Schule überhaupt nicht zuständig ist.

  Nach § 5 Schul-DSVO trägt die BSB die datenschutzrechtliche Gesamtverantwortung für das ZSR und hat damit auch die erforderlichen technischen und organisatorischen Maßnahmen sicherzustellen. Dennoch war sie nicht immer in der Lage, die von uns aufgeworfenen Fragen zu beantworten. Deshalb muss die Prüfung auch im kommenden Berichtszeitraum fortgesetzt werden.

8.4 Data Warehouse der Behörde für Schule und Berufsbildung (BSB)

Die IT-Landschaft der BSB steht vor grundlegenden Veränderungen. Dreh- und Angelpunkt ist dabei die Einrichtung eines Data Warehouses, das noch einige datenschutzrechtliche Fragen aufwirft.

Die BSB hat eine über die Jahre gewachsene IT-Anwendungslandschaft mit sehr unterschiedlichen Systemen. Ein zentraler Zugriff auf diese Systeme ist derzeit nicht gegeben. Es ist bislang auch nicht sichergestellt, dass gelieferte Informationen vergleichbar sind, damit Quantitäts- und Qualitätskennzahlen nicht unterschiedlich dargestellt und interpretiert werden. Dies soll sich ändern, indem eine zentrale Versorgung der Anwendungen mit BSB-weit gültigen Unternehmensdaten aus dem Data Warehouse erfolgen soll. Hierfür hat die BSB das Projekt Data Warehouse installiert.

Durch die uns vorgestellte Data Warehouse-Lösung soll vor allem die Bereitstellung von qualitätsgesicherten Daten in einem geordneten und trans-

parenten Prozess gewährleistet werden. Die für eine Aufgabe erforderlichen Daten werden nach Prüfung der Übermittlungs- und Verarbeitungsbefugnis aus den Quellsystemen angefordert, von dort in ein zentrales Datenhaltungssystem übermittelt und der anfordernden Stelle als Teilkopie aus dem Gesamtbestand zur Verfügung gestellt.

Das Data Warehouse ist ein zentraler Datenspeicher, der Daten aus einer Vielzahl unabhängiger Datenquellen einer unternehmensweiten IT-Landschaft physisch integriert. Datenschutzrechtlich sind damit solange keine Probleme verbunden, wie im Data Warehouse keine personenbezogenen Daten verarbeitet werden, weil hierfür das Datenschutzrecht nicht gilt. Das Modell der BSB sieht aber die Einbeziehung personenbezogener Daten vor, so dass das Data Warehouse der BSB dem Regelungskreis des Datenschutzrechts unterfällt. Zu den Daten mit Personenbezug, die nach gegenwärtigem Stand in das Data Warehouse übernommen werden sollen, gehören im Wesentlichen die Schüler- und Absolventeninformationen für staatliche und nicht-staatliche berufliche und allgemeinbildende Schulen. Diese Daten umfassen auch Informationen zu den jeweiligen Sorgeberechtigten.

Die BSB hat anerkannt, dass das Data Warehouse datenschutzrechtlich relevant ist, und hat dazu eine Verfahrensbeschreibung nach § 9 HmbDSG und eine Risikoanalyse nach § 8 Abs. 4 HmbDSG gefertigt. Diese beiden Dokumente dienten als Einstiegspunkt für die datenschutzrechtliche Betrachtung des Gesamtsystems und verweisen auf die relevanten Verfahrensbeschreibungen und Risikoanalysen der Quellsysteme.

In den Erörterungen mit der BSB haben wir bis ins Detail die Ausprägung des Data Warehouses diskutiert. Beispielsweise haben wir verlangt, dass die lückenlose Dokumentation aller Verwendungszwecke personenbezogener Daten bereits in der Verfahrensbeschreibung des Systems erfolgen muss, in dem die Daten ursprünglich erfasst werden. Liefert ein Verfahren also personenbezogene Daten an das Data Warehouse, so ist es nicht ausreichend, allein die Übergabe an das Data Warehouse zu dokumentieren. Es ist stattdessen notwendig, in der Verfahrensbeschreibung des abgebenden Systems alle Zielsysteme zu dokumentieren, an die die Daten aus dem Data Warehouse weitergegeben werden.

Ebenso haben wir gefordert, dass für jedes einfließende personenbezogene Datum der zulässige Zweck und die Aufbewahrungsfrist definiert und festgelegt und ein geregeltes, datenschutzgerechtes Löschkonzept vorgesehen wird. Über die Aufbewahrungsfristen der Fachverfahren hinaus dürfen die Daten im Data Warehouse nicht mehr personenbezogen oder personenbeziehbar gespeichert bleiben – sondern sind zu löschen. Daten,

welche für statistische, analytische Zwecke über diese Aufbewahrungsfristen hinaus verfügbar gehalten werden müssen, sollten daher von vornherein anonymisiert und separat gespeichert werden.

Außerdem haben wir auf eine sehr genaue Betrachtung der technischen Struktur des Data Warehouses im Rahmen der Risikoanalyse Wert gelegt. Hier ist zu begründen, dass das Gefährdungsrisiko, das durch die zentralisierte Speicherung mehrerer Datenbereiche entsteht, durch geeignete technische und organisatorische Maßnahmen beherrschbar ist.

Grundsätzliche Bedeutung hat die Frage, ob für die Verarbeitung personenbezogener Daten im Data Warehouse eine Rechtsverordnung gemäß § 11a HmbDSG erforderlich ist. Dies ist aus unserer Sicht der Fall, denn nach Absatz 1 Satz 1 dieser Bestimmung bedarf die Einrichtung gemeinsamer und verbundener automatisierter Dateien, in oder aus denen mehrere hamburgische öffentliche Stellen personenbezogene Daten verarbeiten dürfen, der ausdrücklichen Zulassung durch eine Rechtvorschrift. § 11a Abs. 1 Satz 2 HmbDSG ermächtigt den Senat, die Einrichtung solcher Dateien durch Rechtsvorschrift zuzulassen. Wir meinen, dass die verschiedenen Fachbereiche der BSB, die Daten in das Data Warehouse einstellen oder in Empfang nehmen, unterschiedliche Daten verarbeitende Stellen im Sinne des § 4 Abs. 3 HmbDSG sind. Dies entspricht auch dem im Datenschutzrecht allgemein gültigen funktionalen Behördenbegriff. Die BSB dagegen vertritt die Auffassung, sie sei als Ganzes einschließlich ihrer einzelnen Organisationseinheiten datenverarbeitende Stelle. Das bedeutet beispielsweise, dass die Schulen nicht selbständige Daten verarbeitende Stellen sind, was aus unserer Sicht nicht nachvollziehbar ist. Die Diskussion über dieses Thema war bei Redaktionsschluss noch nicht abgeschlossen. Das Ergebnis hat aber zentrale Bedeutung für unsere weitere datenschutzrechtliche Einschätzung des Projektes. Wir hoffen, im nächsten Tätigkeitsbericht eine Lösung präsentieren zu können, die alle Seiten zufrieden stellt.

8.5 Dienstanweisung zum Datenschutz und zur Aktenführung für REBUS

Endlich ist es geschafft, den Datenschutz und die Aktenführung bei den Regionalen Beratungs- und Unterstützungsstellen mit klaren Vorgaben zu versehen.

Regionale Beratungs- und Unterstützungsstellen (REBUS) sind Dienststellen der Behörde für Schule und Berufsbildung (BSB), die ein umfangreiches Hilfesystem bei schulischen Problemen anbieten. Mit der Verarbeitung personenbezogener Daten durch REBUS haben wir uns in den ver-

gangenen Jahren immer wieder auseinandergesetzt (vgl. zuletzt 22. TB, 8.2). Ein Ergebnis dieser Diskussion war eine Dienstanweisung zum Datenschutz und zur Aktenführung für REBUS, die am 12. März 2010 von der BSB in Kraft gesetzt worden ist. Davon erfuhren wir allerdings erst durch Zufall, ohne dass sich die BSB zu den Punkten, die von uns im Rahmen der Abstimmung als klärungsbedürftig angemerkt worden waren, geäußert hatte. Von dieser Vorgehenseise waren wir sehr überrascht und haben dies auch unmissverständlich gegenüber der BSB kritisiert.

In den anschließenden Erörterungen mit der BSB zur allgemeinen Problematik des Schutzes von Klientendaten bei REBUS machten wir deutlich, dass die Dienstanweisung um die für die Klientenberatung grundlegenden Normen ergänzt werden muss, da andernfalls eine einwandfreie Konkretisierung weder zu Maßnahmen des Dienstbetriebs noch zur Datensicherheit möglich ist. Die BSB hat sich daraufhin bereiterklärt, eine Neufassung zu erstellen. Deswegen haben wir darauf verzichtet, die Vorgehensweise der BSB und die damit verbundenen datenschutzrechtlichen Mängel in der Dienstanweisung gemäß § 25 HmbDSG zu beanstanden.

Da es unser Bestreben war, möglich rasch zu einer datenschutzrechtlich einwandfreien Dienstanweisung zu gelangen, haben wir selbst eine konsolidierte Textfassung gefertigt. Dies führte dazu, dass die BSB die Dienstanweisung auf unserer Grundlage noch einmal vollständig überarbeitete. So konnten unsere rechtlichen Bedenken sehr schnell ausgeräumt werden. Nachdem in der Folge noch einige technisch-organisatorische Fragestellungen abschließend mit uns geklärt wurden, hat die BSB die Neufassung der Dienstanweisung zum Ende des Berichtszeitraums dem Personalrat zur Befassung zugeleitet. Zwar lag bis zum Redaktionsschluss noch kein Votum des Personalrats vor, doch wir gehen davon aus, dass es gelingen wird, in Kürze die Neufassung der Dienstanweisung in Kraft zu setzen. Damit wären die bisherigen datenschutzrechtlichen Mängel endgültig geheilt.

8.6 Fragebogenaktionen an Schulen

Die Befragung von Schülern sowie deren Eltern muss anonymisiert erfolgen.

Sowohl die Behörde für Schule und Berufsbildung (BSB) als auch Wissenschaftler möchten in bestimmten Fällen Schüler sowie deren Eltern zu Themen befragen, die beispielsweise für die Entwicklung und Steuerung der Schulen wichtig sein können. So geschah dies auch im Projekt „Aktualisierung des Hamburger Sozialindex“. Die Feststellung der sozialen Zusammensetzung der Schülerschaft der staatlichen Schulen hat eine große Bedeutung für die Steuerung des staatlichen Schulwesens, insbesondere

die angemessene Ausstattung mit Ressourcen. Die Erhebung der Sozialindices der Schulen wurde als eigene Untersuchung der BSB durch das Institut für Bildungsmonitoring durchgeführt. Zentrale Erhebungsinstrumente waren Fragebögen, die an Eltern und deren Kinder ausgegeben wurden.

Die Teilnahme an der Befragung war nicht verpflichtend, sondern freiwillig. Im Fall einer Nichtteilnahme entstanden weder dem Schüler noch den Eltern irgendwelche Nachteile. Vor der Befragung musste eine entsprechende schriftliche Einwilligungserklärung eingeholt werden. Eine bereits erteilte Einwilligung konnte von den Eltern widerrufen werden, solange das Kind den Fragebogen noch nicht ausgefüllt hatte. Durch organisatorische Maßnahmen war sichergestellt, dass keine Daten aus der Befragung in der Schule verbleiben. Das bedeutet insbesondere, dass die Daten nicht zur Schülerakte oder zu sonstigen personenbezogenen Sammlungen des Schülers in der Schule genommen werden durften.

Damit die Fragebögen in der Schule jedem Schüler korrekt zugeordnet und damit auch die Fragebogeninformationen jedes Schülers mit denen der Eltern zusammengeführt werden können, musste jeder Schüler- und jeder Elternfragebogen mit einem individuellen Schüler-Code versehen werden. Der Code bestand aus dem ersten Buchstaben des Vornamens, dem letzten Buchstaben des Vornamens, dem letzten Buchstaben des Nachnamens, dem Geburtstag (zweistellig) und dem Geburtsmonat (zweistellig). So hatte z. B. eine Frederike Braun, geboren am 07.10.1970 die Codenummer FEN0710. Damit war es in vielen Fällen möglich, mit verhältnismäßig geringem Aufwand zu erkennen, um welche Person es sich handelte. Nach der EDV-mäßigen Übernahme der Daten aus den Fragebögen, dem Datencleaning und bestimmten Plausibilitätsprüfungen wurden sofort die individuellen Codes im Datensatz gelöscht. Archiviert wurde nur der Datensatz ohne die individuellen Codes der Schüler, d.h. die Anonymisierung erfolgte erst bei der elektronischen Speicherung der Daten.

Dieses Verfahren entspricht der Praxis von Befragungen, die in den vergangenen Jahren ohne Beanstandungen der Öffentlichkeit und unter unserer Beteiligung in Schulen durchgeführt worden sind. Deshalb haben wir auch diesmal zunächst keine datenschutzrechtlichen Bedenken vorgetragen, so dass die BSB in gutem Glauben gehandelt hat, die Befragung zum Sozialindex sei datenschutzrechtlich in Ordnung. In der Öffentlichkeit entzündete sich aber Kritik insbesondere an der Anonymisierung der Fragebögen. Selbstkritisch müssen wir konstatieren, dass diese Kritik nicht aus der Luft gegriffen war. Deshalb haben wir die Angelegenheit noch einmal an die BSB herangetragen, um zu erreichen, dass zukünftig bei solchen Befragungen eine Form der Anonymisierung gewählt wird, die keine

Zweifel am Datenschutz aufkommen lässt. Konkret bedeutet dies, dass die Anonymisierung künftig bereits bei der Erhebung der Daten erfolgen sollte und der Code keine personenbezogenen Bestandteile aufweisen darf.

Ein weiterer Kritikpunkt war die Rolle der Lehrkräfte, denn die Befragung der Schüler sollte während der Unterrichtszeit stattfinden. Auch wenn die Lehrkraft angewiesen war, die Fragebögen weder während des Ausfüllens noch danach einzusehen, wird sich dies nach unserer Auffassung nicht immer vermeiden lassen. So ist beispielsweise nicht auszuschließen, dass einzelne Schüler Rückfragen an die Lehrkraft richten. Damit würden der Lehrkraft u.U. einzelne Antworten bekannt. Deshalb haben wir angeregt, dass die Schüler ihren Fragebogen nicht in der Schule, sondern zu Hause ausfüllen sollten. Dies hätte auch den Vorteil, dass die Schüler- und Elternfragebögen bereits zu Hause in einen Umschlag gelegt und verschlossen an die Schule gegeben werden könnten. Dann wäre auch der Schüler-Code entbehrlich.

Die Erörterungen mit der BSB waren bei Redaktionsschluss noch nicht abgeschlossen. Wir stehen bereit, um zusammen mit der BSB eine datenschutzgerechte Lösung zu erarbeiten.

8.7 Projekt „Klimaschutz an Schulen“

Auch Projekte, die das Bewusstsein der Schüler für den Klimaschutz stärken sollen, dürfen den Datenschutz nicht außer Acht lassen.

Durch eine Eingabe haben wir davon erfahren, dass vom Projekt „Klimaschutz an Schulen“ des Landesinstituts für Lehrerbildung und Schulentwicklung (LI) der Wettbewerb „Die Klimakasse – Punkten für das Klima!“ im letzten Quartal des Jahres 2011 ausgerichtet werden sollte. Schüler sollten dazu motiviert werden, durch zahlreiche Maßnahmen in ihrem Alltag Kohlendioxyd einzusparen und so zu punkten. Den Gewinnerteams winkten attraktive Klassenfahrten. Der Wettbewerb wurde durch das Unabhängige Institut für Umweltfragen e.V. (UfU e.V.) in Berlin gemeinsam mit dem LI entwickelt.

Die Teilnahme sollte auf freiwilliger Basis online über die Internetseite www.klimakasse.de laufen. Voraussetzung war, dass sich interessierte Lehrer mit ihrer Klasse, einem Fach- oder Wahlpflichtkurs (Mindestgröße 12 Personen) auf der Wettbewerbsseite anmelden. Die Lehrkraft sollte dort ein Klassenpasswort erhalten, mit dem sich die Schüler mit einem eigenen Zugang persönlich registrieren sollten. Dann sollten die Schüler Fragen zu verschiedenen Themenfeldern des Klimaschutzes wie Wärme, Strom, Mobilität, Abfall und Ernährung beantworten. Die Eingaben sollten online

zu Hause, in der Schule oder nach Registrierung am PC unterwegs von jedem internetfähigen Handy gemacht werden.

Datenschutzrechtlich relevant war zum einen der Fragenkatalog. Es wurden u. a. Angaben zum Privatleben der Schüler und zum Verhalten der Sorgeberechtigten erbeten. Beispiele aus der Vielzahl der Fragen:

- An wie vielen Tagen in der Woche isst du Fleisch oder Wurst?
- Kaufst du im Second-hand-Laden?
- Hast du ein Smartphone?
- Wie viel kg Restmüll hat deine Familie letzte Woche weggeworfen?
- Wie viel kg Glas hat deine Familie letzte Woche weggeworfen?
- Sammelt ihr Papier getrennt?

Zum anderen ergaben unsere angestellten Recherchen und Gespräche mit dem LI, dass bei diesem Projekt zumindest beim UfU e.V. personenbezogene Daten verarbeitet werden, und zwar u. a. der Schülername, die E-Mail-Adresse und das Passwort des Schülers, der Lehrername sowie die E-Mail-Adresse, das Passwort und die Telefonnummer des Lehrers. Damit war klar, dass für diesen Wettbewerb das Datenschutzrecht zu beachten ist.

Im Rahmen unserer Beratung haben wir auf datenschutzrechtliche Defizite hingewiesen, die vor dem Start des Wettbewerbs zu beseitigen waren.

So war im Webauftritt die Datenschutzerklärung nicht hinreichend deutlich erkennbar, sondern im Impressum „versteckt“. Außerdem fehlten in der Datenschutzerklärung einige wichtige Informationen.

Die Lehrer sollten vom UfU e.V. nur einen anonymisierten Datensatz erhalten, aber dennoch bestimmte Plausibilitätsprüfungen vornehmen. Das Erfordernis solcher Prüfungen war für uns nicht nachvollziehbar. Insbesondere haben wir aber befürchtet, dass es dadurch im Einzelfall möglich sein wird, Angaben einem bestimmten Schüler zuzuordnen.

Eine wesentliche Forderung von uns war, dass eine rechtswirksame Einwilligung der Eltern vorliegen muss, ohne die eine Teilnahme der Schüler unzulässig ist. Es muss sich um eine informierte und ausdrückliche Einwilligung handeln, die der Schriftform bedarf (vgl. § 5 Abs. 2 HmbDSG). Sofern Eltern keine Rückmeldung geben, darf dies nicht als Einwilligung gewertet werden.

Schließlich haben wir gefordert, die Internetkommunikation über eine SSL-Verschlüsselung abzusichern.

Das LI hat unsere Kritik ernst genommen und zunächst beschlossen, den Start des Wettbewerbs in das Jahr 2012 zu verschieben. Erst nach Aufarbeitung unserer Kritikpunkte und auch nach Zustimmung durch die Elternkammer soll der Wettbewerb beginnen.

9. Gesundheitswesen

9.1 Probleme des Krankenhausinformationssystems des UKE

Die Komplexität der elektronischen Patientendatenverarbeitung im UKE offenbart immer wieder neue datenschutzrechtliche Problempunkte und erfordert eine dauernde Kommunikation mit Verantwortlichen des Klinikkonzerns.

Im 22. Tätigkeitsbericht (III 9.2) hatten wir über unsere datenschutzrechtliche Prüfung des Klinischen Arbeitsplatzsystems SOARIAN im Jahre 2009 und erste Reaktionen des UKE berichtet. Inzwischen ist einiges abgearbeitet, anderes kaum von der Stelle gekommen. Nachfolgend beschränken wir uns auf drei Kernthemen der Patientendatenverarbeitung im UKE.

9.1.1 Konzernübergreifende Patientenakte und Rückgriff auf Vorbehandlungsdaten

Das UKE ist ein Klinikkonzern, dem neben den Zentren mit ihren Kliniken auch privatrechtlich organisierte Behandlungseinheiten als Töchter angehören: die Ambulanzzentrum GmbH, die Martiniklinik GmbH, die Universitäres Herzzentrum GmbH (UHZ) und die AKK Altonaer Kinderkrankenhaus gGmbH. Außer der letztgenannten Klinik befinden sich die Einrichtungen auf dem UKE-Gelände Martinistraße. Sie sind an die zentrale IT-Infrastruktur angeschlossen und dokumentieren ihre Behandlungen in gemeinsamen konzernübergreifenden elektronischen Patientenakten. Diese SOARIAN-Akte ist als „lebenslange“ und umfassende Dokumentation über alle Behandlungsfälle konzipiert. Wer auf die elektronische Patientenakte zugreifen darf, sieht unterschiedslos alle Behandlungsdaten dieses Patienten, egal in welcher rechtlich selbstständigen UKE-Einheit er behandelt wurde, wann er behandelt wurde und welche Krankheit (Behandlungsfall) behandelt wurde.

Das gilt auch für den Zugriff von Organisationseinheiten, die nur zu einem sehr eingeschränkten Zweck auf die Patientendaten zugreifen wie z. B. die Abrechnungsstelle UNIMED, Monitore für bestimmte Forschungsprojekte, Mitarbeiter der MEDIGATE GmbH im Rahmen bestimmter Forschungsprojekte und PJ-Studenten oder Doktoranden. Jeder Zugriff auf die gesamte Patientenakte führt zu einer Offenbarung von sehr viel mehr Daten, als für

die Aufgabenerfüllung erforderlich sind. Hierzu werden wir mit dem UKE weiter im Gespräch bleiben.

Dieses Alles-oder-nichts-Prinzip wird datenschutzrechtlich dadurch verschärft, dass der Patient bereits bei der Aufnahme in einer Klinik des Konzerns gebeten wird, in die „Heranziehung früherer Behandlungsunterlagen“ einzuwilligen (vgl. schon 22.TB III 9.1.).

Wir haben uns mehrfach mit der Frage auseinander zu setzen gehabt, ob das UKE (Konzernmutter wie Töchter) eine Klinikaufnahme ablehnen darf, wenn der Patient diese Einwilligung nicht geben will. Grund dafür kann sein, dass er – wegen negativer Vorerfahrungen – eine unvoreingenommene Diagnosestellung wünscht oder die Patientin nicht möchte, dass der Orthopäde, der den aktuellen Armbruch richtet, auch von einer früheren Abtreibung oder einer längst ausgeheilten Geschlechtskrankheit erfährt. Der vom Patienten bei der Aufnahme zu unterschreibende Behandlungsvertrag sah früher keine Möglichkeit vor, über die Heranziehung der Vorbehandlungsdaten gesondert zu entscheiden. Eine Streichung dieses Passus durch den Patienten hatte zur Folge, dass der Behandlungsvertrag nicht zustande kam, der Patient nicht aufgenommen wurde.

Auf unsere Einwände hin wurde der Behandlungsvertrag geändert und eine Ankreuzmöglichkeit zur Heranziehung von Vorbehandlungsdaten geschaffen. In die Dienstanweisung (SOP) „Ablehnung des Behandlungsvertrages“ wurde aufgenommen, dass – will der Patient keine Heranziehung von Vorbehandlungsdaten – zwischen Arzt und Patient ein Gespräch darüber stattfindet, ob eine Behandlung aus ärztlicher Sicht auch ohne Zugriff auf frühere Behandlungsdaten vertretbar ist. Später wollte das UKE, dass die Aufnahmekraft den Patienten-Ombudsman des UKE verständigt, wenn ein Patient die Einwilligung in die Heranziehung von Vorbehandlungsdaten ablehnt. In einer Buchveröffentlichung von 2011 (Gocke / Debatin: IT im Krankenhaus, S.17 f.) heißt es dagegen wieder: „Verweigert der Patient diese Einwilligung und liegt kein Notfall vor, kann eine elektive *(nicht notfallmäßige)* Behandlung des Patienten nicht erfolgen“. Diese Linie hatte auch der bisherige Vorstandsvorsitzende des UKE immer vertreten, obwohl der Behandlungsvertrag etwas anderes vorsieht.

Nach wie vor sind wir der Auffassung, dass es gegen die datenschutzrechtlichen Grundsätze der Erforderlichkeit, der Datensparsamkeit und der Freiwilligkeit der Einwilligung verstößt, wenn die administrative Klinikaufnahme (außer in Notfällen) von vornherein davon abhängig gemacht wird, dass der Patient in die Heranziehung der umfassenden elektronischen Patientenakte einwilligt.

Neben der Beschränkung des Zugriffs auf die tatsächlich erforderlichen Vorbehandlungsdaten fordern wir auch die sog. „Mandantenfähigkeit“ des Gesamtsystems. Datenschutzrechtlich gibt es kein Konzernprivileg. Jede Daten verarbeitende Stelle, d.h. jede behandelnde Tochter-GmbH des UKE ist für Datenschutz und Datensicherheit selbst verantwortlich. Das Kern-UKE als öffentliche Stelle unterliegt (neben dem HmbKHG) dem Hamburgischen Datenschutzgesetz, die privatrechtlichen Töchter dem Bundesdatenschutzgesetz. Das SOARIAN-System muss dies so nachvollziehen, dass jede rechtlich selbstständige UKE-Einrichtung die Datenverarbeitung einschließlich der Behandlungsdokumentation auch anders als die Konzernmutter durchführen kann – als eigene „Mandantin“ des Systems. Das hindert nicht, dass sich die Töchter der zentralen IT-Abteilung des UKE als Auftragnehmer bedienen, dafür müssen sie aber entsprechende Verträge nach § 9 HmbKHG, § 11 BDSG schließen. Die aus Gründen des Medizinrechts dennoch erforderliche Einwilligung des Patienten in die Übermittlung bzw. Bereitstellung und den Abruf von Patientendaten zu und von anderen UKE-Einheiten muss freiwillig sein. Die Drohung mit einer Nichtbehandlung schränkt die Entschlussfreiheit des Patienten jedenfalls in den vielen Fällen ein, in denen der Patient auf eine Behandlung im UKE angewiesen ist.

9.1.2 Protokollierung von Zugriffen auf Patientendaten

Zur Gewährleistung der Revisionsfähigkeit sind Zugriffe auf elektronische Patientendaten zu protokollieren und die Protokolldaten auszuwerten. Das UKE hat inzwischen ein Auswertungskonzept vorgelegt.

Seit Einführung des SOARIAN-Systems zur Patientendatenverwaltung werden die lesenden und schreibenden Zugriffe auf die einzelnen elektronischen Patientenakten automatisch protokolliert. In zumindest einem Fall hat die Leitung des UKE diese Protokolldaten zur Aufdeckung eines missbräuchlichen Zugriffs auch ausgewertet. Die UKE-Leitung behält sich dies bei jedem aufkommenden Missbrauchsverdacht vor. Gegen diese Praxis wandte sich einer der beiden Personalräte des UKE mit der Begründung, dass es an einem Auswertungskonzept unter Beteiligung des Personalrats fehle.

Zur Gewährleistung der Datensicherheit nach § 8 HmbDSG ist diese verdachtsabhängige Auswertung der Protokolldaten allein jedoch nicht ausreichend. Nicht erst bei einem Verdacht, der meist aus der Verwendung missbräuchlich erlangter Kenntnisse zum Nachteil eines Dritten herrührt, ist die Datensicherheit bedroht. Vielmehr müssen technische und organisatorische Maßnahmen getroffen werden, „die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes *zu gewährleisten“*, § 8 Abs. 1

HmbDSG. Diese positive Gewährleistungspflicht bedingt, dass Protokolldaten auch gezielt und anlassunabhängig nach möglichen Verdachtsmomenten ausgewertet werden. Wir hatten das UKE deswegen schon nach unserer Prüfung im August 2009 aufgefordert, sowohl für die verdachtsabhängige als auch für die anlassunabhängige Auswertung der Protokolldaten ein Konzept vorzulegen. Ohne eine regelmäßige Auswertung wäre eine längerfristige Speicherung von Zugriffsdaten eine unzulässige Vorratsdatenspeicherung.

Erst im Februar 2010 erhielten wir vom UKE zunächst eine Absichtserklärung zur anlassunabhängigen Protokollauswertung, die aber im März wieder zurückgenommen wurde. Wir beharrten auf unserer Forderung und haben Mitte Juli 2011 einen ersten und – auf unsere Reaktion – Ende September 2011 einen differenzierteren Konzeptentwurf zugesandt bekommen.

Danach sollen Zugriffe auf Daten von Prominenten, von Patienten, die eine sog. „Pförtnersperre“ (keine Mitteilung an Außenstehende) haben einrichten lassen, und von Patienten, die zugleich UKE-Mitarbeiter/innen sind und die Kontrolle wünschen, exemplarisch überprüft werden. Im Übrigen sollen stichprobenweise alle Zugriffe eines Monats auf 10 zufällig ausgewählte Patienten zunächst auf ihre Plausibilität und bei Auffälligkeiten bis zu einer User-bezogenen Prüfung untersucht werden. Als auffällig gelten z. B. lediglich einmalige Zugriffe auf einen Patienten und die häufige Nutzung von Suchfunktionalitäten (Ähnlichkeitsabfragen). Zuständig für die Auswertung sind der Abschnittsleiter des Geschäftsbereichs IT und der/die Datenschutzbeauftragte des UKE – nach dem 4-Augen-Prinzip mit geteiltem Passwort. Insbesondere für die User-bezogene Detailauswertung strebt die UKE-Leitung eine Dienstvereinbarung mit den Personalräten an.

Auch wenn auf diese Weise nur ein sehr kleiner Teil der Datenzugriffe kontrolliert wird, haben wir dieses Konzept als ein Instrument akzeptiert, mit dem zunächst Erfahrungen gesammelt werden müssen. Uns ist bewusst, dass mit der systematischen Auswertung von Protokolldaten das UKE Neuland betritt und nur wenige Vorbilder bei anderen Klinika vorfindet.

Hinsichtlich der verdachtsabhängigen, d.h. direkt Mitarbeiter-bezogenen Protokolldatenauswertung bedarf es einer Dienstvereinbarung zwischen der UKE-Leitung und den Personalräten. Wie diese hinsichtlich Verfahren und Kontrollberechtigten im Einzelnen aussehen soll, werden wir nicht vorgeben. Solange ein abgestimmtes Verfahren nicht besteht, bleibt datenschutzrechtlich die UKE-Leitung als Vertretungsorgan der öffentlichen

Stelle Universitäts-Klinikum für den Patientendatenschutz und die Datensicherheit verantwortlich. Sie ist damit befugt und verpflichtet, Missbrauchsvorwürfen auch durch eine Auswertung der Protokolldaten nachzugehen.

9.1.3 Notzugriffe außerhalb des Berechtigungskonzepts

Von der Möglichkeit, auch außerhalb der normalen eigenen Zugriffsberechtigung Patientendaten aufzurufen, wird im UKE unverhältnismäßig oft Gebrauch gemacht. Mit einer Protokolldatenauswertung sollen die Gründe dafür ermittelt und vermindert werden.

Im letzten Tätigkeitsbericht (22.TB, III 9.2) hatten wir den „user contact“ im SOARIAN-System angesprochen – ein außerhalb des normalen Berechtigungskonzepts möglicher Zugriff jedes Arztes / jeder Ärztin auf (alle) Patientendaten, wobei der User auf die Ausnahmefunktion hingewiesen, zur Eingabe einer Freitext-Begründung aufgefordert und über eine automatische Protokollierung des Zugriffs informiert wird. Aufgrund unserer Forderungen (September 2009) nach einem Erfahrungsbericht und einer Protokollauswertung erhielten wir im Februar 2010 eine erste Auswertung der user-contact-Zugriffe für einen Stichtag Ende Januar. Von den 168 Notzugriffen an diesem einen Tag erfolgte die Mehrzahl aufgrund von Prozessablauf- oder Akzeptanzproblemen (OP-Vorbereitung, Konsile, Notaufnahme), aber wahrscheinlich innerhalb des Behandlungszusammenhangs. Der Notzugriff diente angesichts technischer Defizite von SOARIAN der individuellen Verfahrensoptimierung. Nicht nachvollziehbar – und „in der Kürze der Zeit nicht zu verifizieren“ – blieb die Begründung für 26 user-contact-Zugriffe (von ca. 7.000). Dies hielten wir für nicht vertretbar und forderten neben monatlichen Berichten ein effizientes Prüfungskonzept.

In einem Gespräch im März 2010 machten der Vorstandsvorsitzende des UKE und weitere Verantwortliche folgende Zielvorgaben für eine Reduzierung des Anteils von user-contact-Zugriffen an der Gesamtzahl der Zugriffe: 0,2 % bis Ende 2010 und 0,1 % bis Ende Juni 2011.

Der Ende Juni 2010 übersandte zweite Auswertungsbericht für Mai 2010 ergab in dem Monat mehr als 5000 user-contact-Zugriffe (bei knapp 1,3 Mio. Zugriffen insgesamt, Anteil: 0,4 %), durchschnittlich mehr als 200 pro Tag. Im Oktober 2010 wurden 6400 user-contact-Zugriffe registriert (Anteil ca. 0,4 %), davon über 1300 ohne plausible Begründung. Eine stichprobenweise Auswertung der angegebenen Zugriffsgründe erfolgte dieses Mal entweder nicht oder wurde uns nicht zur Kenntnis gegeben. Im Okto-

ber 2010 erhielten wir ein Prüfungskonzept in Form eines Entwurfs einer Dienstvereinbarung mit dem wissenschaftlichen Personalrat WPR.

Da uns weder die mehrfach erbetenen monatlichen Auswertungsübersichten erreichten, noch der Abschluss einer entsprechenden Dienstvereinbarung gemeldet wurde, haben wir uns im Februar 2011 im UKE die Datei der user-contact-Zugriffe mit den verschiedenen auswertungsfähigen Merkmalen zeigen lassen. Dem vorgeschlagenen mehrstufigen Prüfungsverfahren nach verschiedenen Kriterien haben wir grundsätzlich zugestimmt. Dennoch haben wir seit über einem Jahr keine Dateiauswertung der user-contact-Zugriffe mehr bekommen. Im April 2011 teilte uns das UKE mit, man habe sich „auf die Begrifflichkeit „Sonderzugriffsmöglichkeit“ statt „Notzugriff““ verständigt, da es in weiteren eng umgrenzten Fällen „Ausweichmöglichkeiten“ von dem recht rigiden Berechtigungskonzept bedürfe. Trotz weiterer Diskussionen des Dienstvereinbarungsentwurfs – ein neuer Entwurf folgte im Juli 2011 – ist es bisher nicht zu einem Abschluss gekommen.

Wir halten die Möglichkeit, auf sensibelste Patientendaten außerhalb des aufgabenbezogenen Berechtigungskonzepts zuzugreifen, grundsätzlich für eine Gefährdung des informationellen Selbstbestimmungsrechts wie auch der ärztlichen Schweigepflicht. Ziel muss es sein, die Notzugriffe auf ein Minimum zu reduzieren – etwa durch Behebung von Prozessablauf-, Schnittstellen- und Akzeptanzproblemen, aber auch durch eine abschreckende Wirkung nachhaltiger Kontrollmaßnahmen. Die äußerst langwierige Behandlung des Problems im UKE erscheint uns nicht angemessen. Da der Vorstandsvorsitzende selbst an wesentlichen Gesprächen teilnahm, erschien uns eine offizielle Beanstandung nach § 25 HmbDSG wenig erfolgversprechend. Wir werden aber auch weiterhin auf datenschutzgerechte Schutzmaßnahmen gerade in diesem Bereich drängen.

9.1.4 Remotezugriffe im KIS-II-Netz

Die Bedingungen für die administrativen Zugriffe auf PC im UKE konnten datenschutzgerecht umgestaltet werden. Den Nutzern konnte der Einblick in die aktuellen Zugriffsrechte ihrer Dateien allerdings nicht realisiert werden.

Bereits Ende 2009 haben wir aus gegebenem Anlass eine Prüfung der Remote-Administration im KIS-II-Netz des UKE begonnen. Das KIS-II-Netz ist ein vom KIS-I-Netz, in dem die Patientendatenverarbeitung erfolgt, getrenntes Bürokommunikationssystem des UKE mit mehreren hundert PC. Es dient zur Erstellung des allgemeinen Schriftverkehrs und kann dabei im Einzelfall auch personenbezogene Daten enthalten. Für die zentrale Administration dieses Netzes wird eine Software eingesetzt, die es Mitarbeitern

des Geschäftsbereichs IT ermöglicht, sich auf die einzelnen PC der Nutzer aufzuschalten. An uns wurden Hinweise herangetragen, dass es bei der Nutzung dieser Software zu Unregelmäßigkeiten gekommen war.

Zum Zeitpunkt unserer Prüfung stellte sich die Situation wie folgt dar:

1. Für die Remote-Administration wird die Software „Dameware“ genutzt. Diese ist auf den Geräten der KIS-II-Administratoren installiert und ermöglicht verschiedene administrative Tätigkeiten auf den KIS-II-PC. Hierzu gehört die Aufschaltung auf den Bildschirm des an einem KIS-II-PC angemeldeten Nutzers.
2. Eine solche Aufschaltung erfolgt regelmäßig anlassbezogen auf Nutzeranruf hin; der Nutzer muss dabei die Aufschaltung durch Mausklick bestätigen. Allerdings ist es möglich, die Erforderlichkeit der Nutzerbestätigung auszuschalten. Dies können alle Dameware-Nutzer im UKE tun, da die Konfiguration, mit der die Bildschirmaufschaltung gestartet wird, bei jeder einzelnen Aufschaltung geladen wird und nicht fest auf dem fernen PC hinterlegt ist. Vielmehr wird der Teil der Software, die auf dem zu wartenden PC für eine Bildschirmaufschaltung erforderlich ist, jeweils zunächst dorthin geladen und ein entsprechender Dienst gestartet. Erst dann erfolgt die konkrete Aufschaltung – unter Verwendung der zuvor mitgegebenen ggf. angepassten Einstellungen.
3. Die Bildschirmaufschaltung wird lokal auf den entsprechenden PC protokolliert. Die Windows-Protokolldateien haben im KIS-II-Bereich die Standardgröße 512 kB. Eine zentrale Protokollierung findet nicht statt.
4. Insgesamt 11 Administratoren des Geschäftsbereichs IT haben einen Dameware-Zugang. Einer der Accounts besteht für Testzwecke.

Hierbei war eine Reihe datenschutzrechtlicher Probleme erkennbar, die vor allem aus der mangelnden Nachvollziehbarkeit der administrativen Tätigkeiten resultierten. Die Möglichkeit einer im Einzelfall für den Nutzer nicht erkennbaren Aufschaltung eröffnet erhebliche Missbrauchspotenziale. Wir haben daher gefordert, dass die Remote-Administration in einem geregelten, nachvollziehbaren Verfahren erfolgen muss. Hierzu gehört, dass ein Aufschalten nur möglich ist, wenn der Nutzer zugestimmt hat und sich diese Zustimmung nicht umgehen lässt. Zudem ist eine revisionssichere Protokollierung erforderlich, die administrative Tätigkeiten an zentraler Stelle nachvollziehbar dokumentiert.

Das UKE hat auf unsere Anforderungen reagiert, indem die Nutzung von Dameware über einen Terminalserver kanalisiert wird. Die KIS-II-PC nehmen nur Administrationsanfragen dieses Servers an, auf dem eine feste Dameware-Konfiguration hinterlegt ist. Die einzelnen Administratoren, die sich über diesen Weg auf PC aufschalten, haben nicht die Möglichkeit, die

Konfiguration zu ändern. Eine Deaktivierung der Nutzerbestätigung ist ihnen daher nicht mehr möglich. Zugleich erfolgt eine zentrale Protokollierung der Aufschaltungen. Diese haben wir im Rahmen einer Nachprüfung im 4. Quartal 2011 kontrolliert.

Ergänzend zu diesen Maßnahmen wurde eine neue SOP zur Fernwartung im UKE erstellt, die Menge der Dameware-Nutzer bereinigt sowie eine Software in Betrieb genommen, die es ermöglicht, individuelle administrative Passwörter auf den KIS-II-PC zu verwalten. Dies vermeidet, dass bei unberechtigtem Bekanntwerden des administrativen Passworts eines Geräts sämtliche anderen Geräte angepasst werden müssten.

Im Zuge unserer Prüfung haben wir einen weiteren Themenbereich angesprochen, der aus unserer Sicht datenschutzrechtlich verbesserungsbedürftig ist.

Jeder KIS-II-Nutzer hat Zugriff auf zentrale Gruppenlaufwerke, deren Rechte je nach Anforderung und Arbeitsorganisation gesetzt sind. Für die Bereitstellung dieser Laufwerke verwendet das UKE Novell-Dateidienste, die in die Windows-Umgebung der PC eingebunden werden.

Die KIS-II-Nutzer haben dabei weder die technische Möglichkeit, die Zugriffsrechte zu ändern, noch sich über die Zugriffsrechte der Ordner und Dateien zu informieren, die ihnen zur Verfügung gestellt werden. Dies haben wir kritisiert und gefordert, dass es zumindest möglich sein muss, die Rechte einzusehen.

Das UKE hat versucht, dies in Kooperation mit dem Hersteller umzusetzen. Dabei hat sich jedoch gezeigt, dass das verwendete Produkt es nicht zulässt, den Nutzern Einblick in die Dateirechte zu geben, ohne dass sie auch weitreichende Rechteänderungsmöglichkeiten bekommen, die weit über das Erforderliche und Zulässige hinausgehen. Die Nutzer wären dann in der Lage, auch in fremde Verzeichnisse Einblick zu nehmen, was natürlich verhindert werden muss.

Kompensierend informiert das UKE die Nutzer im Intranet über die Sachlage und bietet in diesem Zusammenhang jedem Nutzer an, sich gemeinsam mit einem Mitarbeiter des Geschäftsbereichs IT über die aktuelle Rechteeinstellung kundig zu machen sowie bei Änderungswünschen zu unterstützen.

9.2 UKE-Therapiezentrum für Suizidgefährdete

Durch die Integration des Therapiezentrums für Suizidgefährdete (TZS) in die Klinik für Psychiatrie und Psychotherapie und in das elektronische Krankenhausinformationssystem des UKE vervielfältigten sich die Möglichkeiten,

auf Patientendaten zuzugreifen. Sie wurden datenschutzgerecht eingeschränkt.

Noch Ende 2009 antwortete der Senat auf eine Schriftliche Kleine Anfrage, dass im Therapiezentrum für Suizidgefährdete (TZS) des UKE insgesamt 4,5 Vollkräfte als Ärzte, Psychologen und Dokumentationsassistenten eingesetzt seien und nur diese Zugriff auf die Behandlungsdaten von Patientinnen und Patienten hätten (Bü-Drs.19/4496). Weitere Personen hatten nur Zugriff auf die Information, dass der Patient einmal im TZS behandelt wurde. Zugleich teilte der Senat mit, dass das TZS in das zentrale klinische Dokumentationssystem SOARIAN des UKE integriert werden sollte.

Dies haben wir zum Anlass genommen, das UKE zu fragen, wie viele Personen im UKE nach der Integration in SOARIAN auf die Behandlungsdaten der TZS-Patienten zugreifen können. Die Antwort hat uns schockiert: Es seien 394 Beschäftigte der Fachrichtung Erwachsenenpsychiatrie – Ärzte, Pfleger und Funktionskräfte. Es werde jedoch geprüft, ob die Zugriffsmöglichkeiten durch eine neue Berechtigungsrolle „TZS-PSY“ eingeschränkt werden könne. In einem Schreiben an den Vorstandsvorsitzenden des UKE haben wir eine solch hohe Berechtigtenzahl als nicht vertretbar kritisiert und eine unverzügliche Umsetzung der Zugriffsbegrenzung gefordert. Daraufhin teilte uns das UKE mit, dass der Zugriff „noch heute“ auf acht Beschäftigte (Ärzte, Pfleger) beschränkt wird. Erst danach erhielten wir die Korrektur, dass nicht 394 Beschäftigte, sondern „nur“ 70 Oberärzte, Assistenzärzte und Psychologen Zugriff gehabt hätten, wozu allerdings stationsbezogen noch die Pflegekräfte hinzuzurechnen waren. Durch Konsilanfragen, Administratorenrechte und im Case-Management können im Einzelfall und individuell weitere Zugriffsberechtigte hinzukommen.

Schon bei der Prüfung des SOARIAN-Systems hatten wir erreicht, dass psychiatrischen und psychotherapeutischen Dokumenten eine Sonderrolle eingeräumt wurde: Auch bei einer Berechtigung zum Zugriff auf die Patientenakte können diese besonders sensiblen Dokumente nur von psychiatrischem und psychologischem Fachpersonal geöffnet werden.

Die bisherige Möglichkeit, Suizidgefährdete auch anonym zu behandeln, wird durch die Integration des TZS in das zentrale Abrechnungs- und Verwaltungsverfahren allenfalls als seltene Ausnahme – unter Pseudonym – beibehalten werden können.

Seit langem kritisieren wir grundsätzlich, dass etwa bei der administrativen Patientenaufnahme ins UKE immer auch ein früherer Behandlungsort mitgeteilt wird, der wie in diesem Fall ein besonders sensibles Datum sein kann. Dies erscheint nur erforderlich, wenn eine laufende Behandlung im UKE noch nicht abgeschlossen ist und die Aufnahme dieser Behandlung

zugeordnet werden muss. Im Übrigen stellt sich die Frage nach einer Vorbehandlung im UKE jedoch erst bei der medizinischen Aufnahme. Bisher hat das UKE diese – nun auch bundesweit formulierte – Forderung der Aufsichtsbehörden, auf eine regelhafte Offenbarung einer funktionellen Organisationseinheit einer früheren Behandlung zu verzichten, nicht umgesetzt (vgl. unten 9.9).

9.3 UKE-Tumorzentrum – Klinisches Krebsregister und Tumorkonferenzen

In intensiver Zusammenarbeit konnte für das Klinische Krebsregister, das zugleich Dokumentation- und Forschungsaufgaben erfüllen soll, eine datenschutzgerechte Struktur gefunden werden. Bei den Tumorkonferenzen ging es vor allem um die Einwilligung der Patienten und eine Beschränkung der vielen Datenzugriffsrechte.

Das „Hubertus Wald Tumorzentrum – Universitäres Cancer Centrum Hamburg“ (UCCH) strukturierte ab 2009 sein Krebsregister neu, um insbesondere die Krebsforschung zu verbessern. Die Herausforderung lag vor allem darin, einerseits eine strukturierte Behandlungsdokumentation aus der elektronischen Patientenakte zu generieren und zu pflegen, andererseits der Forschung nur pseudonyme Daten zur Verfügung zu stellen und dennoch im Bedarfsfall eine – möglichst eingeschränkte – Re-Identifikation für eng umschriebene Aufgaben zuzulassen.

Erreicht wurde dies durch eine Trennung von Importtabelle (Eingang namensbezogener klinischer Daten aus dem Behandlungsbereich des gesamten UKE und externer Partner), einem gesonderten Sicherheitsbereich „Schlüsseltabelle“ und dem eigentlichen Krebsregister ohne Namensbezug. Die Schlüsseltabelle verwandelt die persönlichen Identifikationsdaten der Patienten automatisch in ein Pseudonym und gibt dieses an die Importtabelle zurück. Aus dieser werden die Daten nur mit dem Pseudonym in die Registerdatenbank überführt und in der Importtabelle umgehend gelöscht. Kern des Krebsregisters ist ein ausführlicher standardisierter Datensatz für jeden Patienten. Diese pseudonymisierten Daten kann sowohl die Forschung als auch die Qualitätssicherung nutzen. Die Forscher haben grundsätzlich keinen Zugriff auf die Schlüsseltabelle, mit deren Hilfe die Pseudonyme zu Klarnamen aufgelöst werden können.

Es gibt jedoch Anlässe, bei denen vorübergehend der Personenbezug wieder hergestellt werden muss: so z. B. für die Meldung und für Anfragen beim Hamburgischen Krebsregister, das nach dem Hamburgischen Krebsregistergesetz mit Einwilligung der Betroffenen namensbezogen geführt wird. Aber auch um die personenbezogenen Behandlungs(Diagnose-)pro-

ben in der Pathologie einzubinden, die elektronische Patientenakte mit Erkenntnissen aus der Forschung zu ergänzen oder Probanden für Studien zu gewinnen, die einen Kontakt mit den Patienten erfordern, ist eine kurzfristige Re-Identifikation notwendig. Auch wenn der Patient wissen will, was über ihn im Krebsregister gespeichert ist, bedarf es einer Re-Identifizierung. Damit diese nicht die Pseudonymisierung insgesamt gefährdet, obliegt die Entschlüsselung ausschließlich Mitarbeitern außerhalb des eigentlichen Krebsregisters.

Diese Verarbeitung der Patientendaten im Klinischen Krebsregister ist vom Behandlungsvertrag nicht gedeckt, sie bedarf deswegen einer Einwilligung der Patienten. Das UCCH übernahm unseren Formulierungsvorschlag für Patienteninformation und Einwilligung, der einen Kompromiss zwischen Verständlichkeit, Übersichtlichkeit und ausreichender Unterrichtung anstrebt. Die Erteilung bzw. die Verweigerung oder das Fehlen der Einwilligung wird sowohl im SAP-Verwaltungssystem als auch in der SOARIAN-Patientenakte elektronisch vermerkt und steuert das weitere Verfahren. Verweigert der Patient die Einwilligung für das Klinische Krebsregister, wird ein anonymer Minimal-Datensatz gebildet, um die Vollständigkeits- und Qualitätskontrolle zu ermöglichen.

Mit einer wichtigen Quelle des Klinischen Krebsregisters haben wir uns intensiver beschäftigt: mit den Tumorkonferenzen bzw. den interdisziplinären „Tumorboards“ des UCCH. Jeder Krebsverdacht in einer UKE-Klinik oder bei einer externen Partnereinrichtung wird im UCCH mündlich einem Gremium von Spezialisten verschiedener Fachrichtungen vorgestellt. Als Ergebnis gibt diese Tumorkonferenz der behandelnden Einrichtung eine Therapieempfehlung.

Da die Tumorkonferenzen in aller Regel ohne Anwesenheit des Patienten, aber unter Darstellung von vorab übermittelten Behandlungsunterlagen stattfinden, musste bei den externen Partnereinrichtungen einschließlich der selbstständigen UKE-Töchter die vorherige Einwilligung der Patienten sichergestellt werden. Für Patienten des Kern-UKE selbst gehören die Tumorkonferenzen dagegen zum normalen Behandlungspfad und sind in der medizinischen Aufklärung und gemeinsamen Therapieentscheidung enthalten; einer gesonderten schriftlichen Einwilligung bedarf es hier nicht. Bei den Einwilligungen der Einrichtungen außerhalb des Kern-UKE haben wir nicht akzeptiert, dass diese bereits vorab und vorsorglich im allgemeinen Behandlungsvertrag stehen und mit unterzeichnet werden. Als Mindestvoraussetzung für das Einholen einer Einwilligung haben wir den Verdacht einer Krebserkrankung gefordert. Das UCCH gibt den externen Einrichtungen Muster von Patientenaufklärung und -einwilligung vor und

verpflichtet die Partner vertraglich, nur Patienten vorzustellen, die eine Einwilligung erteilt haben.

Die Behandlungsdaten der Patienten werden den Beteiligten der Tumorkonferenz über das Klinikinformationssystem SOARIAN – „Leistungsstelle Tumorboard“ – zur Verfügung gestellt und noch einmal in der Konferenz per Beamer gezeigt. Soweit die Patienten UKE-Patienten sind oder von externen Einrichtungen an das UCCH überwiesen werden, finden die Dokumente und die Therapieempfehlung auch Eingang in die elektronischen Patientenakte des UKE. Das gilt auch für Patienten, die weiterhin nur in der externen Einrichtung behandelt werden. Diese Datenspeicherung muss deswegen Teil der Aufklärung und Einwilligung sein. Einer weiteren Einwilligung bedarf dann die Übernahme der klinischen Daten und Therapieempfehlung in das Klinische Krebsregister des UCCH (s.o.).

Ein besonderes Problem der Interdisziplinarität der Tumorkonferenzen ist die große Zahl der Zugriffsberechtigten: 208 Personen haben regelmäßig Zugriff auf die „Leistungsstelle Tumorboard“, weitere Personen wie Auszubildende und ggf. Techniker bekommen die Daten bei der Konferenz über die Beamer-Präsentation zur Kenntnis. Hier haben wir Kritik angemeldet und die Zusage einer Zugriffsdifferenzierung erhalten, die angesichts der vielen jeweils betroffenen Fachdisziplinen allerdings keine besonders weitgehende Beschränkung erreichen könne. Wir bleiben mit dem UCCH hierüber in der Diskussion.

9.4 Prüfung eines Facharztzentrums

Bei einem großen orthopädischen Facharztzentrum wurden gravierende Mängel beim Patientendatenschutz festgestellt und zu ihrer Behebung sowohl kurzfristige Einwilligungslösungen als auch längerfristige Systemumstellungen vereinbart.

Aufgrund einer Patientenbeschwerde haben wir Ende 2010 ein größeres Facharztzentrum geprüft. Dies vereinigt unter einem einheitlichen Namen eine Facharzt-Gemeinschaftspraxis für Privatpatienten einschließlich einer Praxis für Psychologie, eine Facharztpraxis für gesetzlich Versicherte und drei eigenständige therapeutische GmbH. Patienten werden von den Praxisärzten entweder abschließend behandelt oder an eine der GmbH überwiesen bzw. von diesen mit- oder weiterbehandelt. Patienten können aber auch von externen Arztpraxen direkt an eine der GmbH des Zentrums überwiesen werden. Insgesamt arbeiten ca. 150 Mitarbeiterinnen und Mitarbeiter in dem Zentrum.

Neben kleineren Mängeln haben wir vor allem die technische Infrastruktur, das elektronische Kommunikationsnetz in dem Zentrum kritisiert: Jeder

Arzt und Therapeut und sehr viele Funktionskräfte hatten Zugriff auf die Behandlungsdaten jedes Patienten in dem Zentrum – unabhängig davon, in welcher Einheit des Zentrums der Patient behandelt wird. Einige Mitarbeiter des Zentrums waren sowohl behandelnden Anwendergruppen als auch zugleich IT-Administratorgruppen zugeordnet. Allein 14 Mitarbeiter hatten Administratorrechte, die z. B. „Befund validieren", „neue Arztbriefe generieren" und „Personalverwaltung" umfassten.

Es gab weder eine „Mandantenfähigkeit" des Systems – also die funktionelle Trennung der einzelnen rechtlich selbstständigen Einheiten –, noch wurden die Patienten über diese weitgehende Verfügbarkeit ihrer Behandlungsdaten aufgeklärt oder um eine entsprechende Einwilligung gebeten. Da es keinerlei Sicherung z. B. gegen den Zugriff eines Mitarbeiters einer nicht beteiligten GmbH auf medizinische Daten von Patienten der Arztpraxen gab, haben wir hierin einen strafbaren Verstoß gegen die ärztliche Schweigepflicht sowie subsidiär eine Ordnungswidrigkeit nach § 43 BDSG gesehen.

Mehr als an einer strafrechtlichen Verfolgung lag uns an einer möglichst baldigen Behebung der Mängel. Das Facharztzentrum sagte eine grundlegende Änderung ihrer elektronischen Infrastruktur zu. Es wird eine technische Möglichkeit entwickelt, mit der der Patient selbst durch die Nutzung einer Code-Karte anderen als den aktuell behandelnden Personen bei Bedarf den Zugang zu seinen Daten eröffnet. Eine solche Lösung dient der informationellen Selbstbestimmung der Patienten in besonderem Maße.

Da eine solche Neuentwicklung für das Zentrum jedoch einige Zeit in Anspruch nimmt, haben wir darauf gedrungen, in der Übergangszeit für die Patienten Transparenz hinsichtlich der technischen Infrastruktur des Zentrums herzustellen und sie um eine Einwilligung zum Datenzugriff zu bitten. In die Einwilligung wurde auch die Fernwartung durch den IT-Dienstleister, die Abrechnung privatärztlicher Leistungen durch eine externe Verrechnungsstelle sowie der Datenaustausch mit dem Hausarzt einbezogen. Dokumente der psychologischen Praxis werden dagegen von der allgemeinen Einwilligung ausgenommen und bedürfen für den Fall der notwendigen Weitergabe einer besonderen Einwilligung im Einzelfall.

Während der Patient die Datenweitergabe an die Verrechnungsstelle ablehnen kann – mit der Folge, dass das Zentrum selbst abrechnet –, ist die Einwilligung in die Datenzugriffe durch die anderen behandelnden Einheiten konstitutiv für die Aufnahme zur Behandlung (vgl. unten 9.7). Durch Verpflichtung auf das Datengeheimnis und eine Anweisung, die technische Zugriffsmöglichkeit nur in Fällen medizinischer Erforderlichkeit

(Überweisung, Mitbehandlung) zu nutzen, wird das Missbrauchsrisiko normativ eingeschränkt. Dennoch haben wir deutlich gemacht, dass erst die geplante technische Option der individuellen Zugriffsfreigabe durch den Patienten die datenschutzrechtlich optimale Lösung darstellt. Für eine Übergangszeit haben wir die Einwilligungslösung akzeptiert und bei der Formulierung von Aufklärung und Einwilligungstext Hilfestellung geleistet. Wir hoffen, im nächsten Tätigkeitsbericht das neue patientenorientierte Zugriffsberechtigungskonzept vorstellen zu können.

9.5 Gutachten des Medizinischen Dienstes der Krankenkassen (MDK): Ergebnis und Befunde

Seit längerem diskutieren wir mit dem MDK die Frage, welcher Teil der sozialmedizinischen Gutachten als Ergebnis und erforderliche Befunde an die Krankenkassen übermittelt werden müssen und dürfen. Bisher steht ein befriedigendes Ergebnis aus.

Seit dem Jahre 1998 gibt es zwischen den Datenschutzbeauftragten und den Medizinischen Diensten der Krankenversicherung (MDK) eine Auseinandersetzung darüber, in welchem Umfang ein vom MDK erstelltes Gutachten an die beauftragende Krankenkasse und ggf. die betroffenen Leistungserbringer (Ärzte, Krankenhäuser) übermittelt werden darf. Nach § 277 Abs. 1 SGB V hat sich die Mitteilung des MDK auf „das Ergebnis der Begutachtung“ und „die erforderlichen Angaben über den Befund“ zu beschränken. Dissens gab es z. B. in der Frage, ob „Befunde“ auch die Anamnese umfassen. Im Ergebnis zog sich der MDK darauf zurück, dass nur im Einzelfall entschieden werden könne, welche Befunde für die Krankenkasse zur Begründung ihrer Entscheidung erforderlich sind.

Die Eingabe einer Bürgerin hat uns wieder auf die Problematik aufmerksam gemacht und zu einer erneuten Auseinandersetzung mit dem MDK geführt. Begutachtet wurde der Wunsch nach Kostenübernahme für eine operative Brustverkleinerung. Das Gutachten gliedert sich in mehrere Kapitel. In der „Vorgeschichte / Anamnese“ war u. a. vermerkt: ein Kind geboren, 2 Jahre gestillt, z.Zt. keine hormonelle Behandlung, Nichtraucherin, „Alkohol nicht“, bekannte Latex-Allergie und Hausstaubmilbenallergie, bekannte Neurodermitis, keine Vor-Operationen. Im „Befund“ wurden alle erdenklichen Größen- Abstands-, Gewichtsangaben zur Brust erfasst – einschließlich der Trägerbreite des BH. Unter Diagnosen waren „Rückenschmerzen im HWS-/BWS-Bereich“ und „Hinweis auf eine Skoliose“ angegeben.

Anhand dieses Beispiels haben wir dem MDK deutlich gemacht, dass wesentliche Teile des Kapitels „sozialmedizinische Beurteilung“ für eine

Entscheidung der Krankenkasse vollständig ausgereicht hätten. Denn in dieser Beurteilung wurden die entscheidenden Sachverhalte aus der Anamnese und dem Befund wieder aufgenommen und bewertet. Eines Nachvollzugs der cm-genauen Brustvermessung bedurfte es für die Entscheidung der Krankenkasse ebenso wenig wie der anderen genannten Angaben aus der Anamnese. Wichtig war allein, ob die Wirbelsäulenbeschwerden und entzündlichen Stellen durch die gewünschte Operation gebessert werden und damit medizinisch indiziert sind, was begründet verneint wurde. Dagegen finden auch die in der sozialmedizinischen Beurteilung angestellten weitergehenden Überlegungen zu körperlicher Auffälligkeit, „regelwidrigem Körperzustand“ und „Entstellung mit Krankheitswert“ weder im Auftrag der Krankenkasse noch in den Angaben und Wünschen der Versicherten selbst eine Begründung. Die Versicherte hatte optische (und psychische) Gründe gar nicht vorgetragen.

Anhand eines weiteren – stattgebenden – Gutachtens zur Arbeitsunfähigkeit haben wir die Unterscheidung in erforderliche und nicht erforderliche Befunde weiter vertieft. Dennoch folgte der MDK dem nicht und lehnte eine eindeutige Gutachten-Aufteilung in mitteilungsbedürftige und darüber hinausgehende Teile ab. Vielmehr erläuterte er, dass immer auch Angaben aus der Anamnese erforderliche Befunde im Sinne des § 277 SGB V seien und erklärte, dass bereits das gesamte Gutachten auf das Maß der „erforderlichen Angaben zum Befund“ beschränkt werde. Es sei aber nicht ausgeschlossen, dass im Einzelfall auch einmal dagegen verstoßen werde.

Da es sich bei den MDK-Gutachten aus unserer Sicht vielfach um sehr sensible, aber für die Entscheidung der Krankenkasse nicht erforderliche personenbezogene Daten handelt, beabsichtigen wir, die Diskussion weiter zu führen und durch die Prüfung weiterer Gutachten vor Ort einem datenschutzrechtlich befriedigenden Ergebnis zuzuführen. Auch bundesweit wollen wir die Auseinandersetzung um die Übersendung vollständiger MDK-Gutachten an Kassen und Leistungserbringer wieder aufnehmen. Als Reaktion auf unsere Problemdarstellung hat uns inzwischen der Medizinische Dienst des Spitzenverbands Bund der Krankenkassen (MDS) in Essen mitgeteilt, dass eine bundesweite Arbeitsgruppe von MDK-Datenschutzbeauftragten mit der Erarbeitung einer Leitlinie zur Umsetzung des § 277 SGB V beauftragt wurde.

9.6 Verweigerung der Behandlung bei Ablehnung von Patienteneinwilligungen

Übermittlungen von Patientendaten zwischen Gesundheitseinrichtungen bedürfen oft der Schweigepflichtentbindung bzw. der datenschutzrechtlichen Einwilligung. Diese durch eine Androhung der Behandlungsverweigerung zu erzwingen, widerspricht vielfach der informationellen Selbstbestimmung der Patienten.

Die zunehmende elektronische Vernetzung im Gesundheitswesen sichert den Praxen und Kliniken eine schnelle Informationsbereitstellung. An die Stelle von individuellen Datenübermittlungen im Einzelfall treten oft Infrastrukturen mit Zugriffs- bzw. Abrufberechtigungen (siehe oben 9.1.1, 9.5). Dazu werden Patienten vielfach um Schweigepflichtentbindungen bzw. Einwilligungen gebeten. Es mehren sich Beschwerden von Patienten darüber, dass ihnen die Behandlung versagt wird, wenn sie diese Einwilligungen nicht erteilen. Dies ist sowohl bei niedergelassenen Ärzten und in einem medizinischen Versorgungszentrum vorgekommen, als auch bei einem privatärztlich abrechnenden UKE-Arzt und in einer Asklepios-Klinik. Es ging um die Zustimmung zum Datentransfer an eine externe Abrechnungsstelle, aber auch um die Einwilligung in die Datenoffenbarung an über 40 externe Dienstleister eines Krankenhauses.

Im Fall der Datenübermittlung an eine Verrechnungsstelle ist die ärztliche Behandlung inhaltlich nicht auf diese angewiesen. Die Erzwingung der externen Abrechnung durch die Versagung der Behandlung stellt deswegen die notwendige Freiwilligkeit der Einwilligung in Frage und verstößt gegen das Koppelungsverbot, das die Literatur aus § 4a BDSG ableitet. Die in der Berufsordnung normierte „Behandlungsfreiheit“ des Arztes gibt diesem keine Ermächtigung zu willkürlicher Entscheidung, sondern nur zu einer sachlichen, rational nachvollziehbaren Abwägung. Der Arzt ist berufsrechtlich an ethische Grundsätze und die Selbstbestimmung des Patienten gebunden. Übt der Patient sein Datenschutzrecht in Form der Verweigerung einer freiwilligen Einwilligung aus, gibt das dem Arzt für sich genommen keinen sachlichen Grund für eine Behandlungsverweigerung. Verwaltungskräfte von Gesundheitszentren und Kliniken – z. B. bei der Aufnahme, am Empfang – können die berufsrechtliche Behandlungsfreiheit eines Arztes bei der Aufnahmeverweigerung ohnehin nicht für sich in Anspruch nehmen.

Die Einwilligung in Datenübermittlungen im Rahmen eines Krankenhaus- oder sogar Konzern-weiten Kommunikationsnetzes mag stärker der interdisziplinären und integrativen Behandlung selbst dienen und damit nicht dem Koppelungsverbot unterfallen. Dennoch ist grundsätzlich an der Freiwilligkeit der Patientenentscheidung festzuhalten. Hat der Patient keine zu-

mutbare Alternative zu der Behandlung in der Einrichtung, die die Einwilligung abfordert, so ist diese nicht freiwillig und damit auch nicht wirksam erteilt.

In vielen Fällen bedarf es im Übrigen gar keiner formellen Einwilligung des Patienten. So können Kliniken z. B. häufig auf gesetzliche Übermittlungsbefugnisse im Hamburgischen Krankenhausgesetz (§ 11) zurückgreifen. In anderen Fällen ist zu prüfen, ob nicht bereits der Behandlungsvertrag und die Abstimmung des weiteren Behandlungsweges mit dem Patienten eine ausreichende Grundlage für entsprechende begleitende Datenweitergaben darstellt. Schließlich ist – gerade bei der Einschaltung externer Dienstleister durch ein Krankenhaus – auch die Figur der Auftragsdatenverarbeitung zu berücksichtigen (§ 9 HmbKHG). Danach liegt bei technischen Hilfstätigkeiten und (Fern-)Wartungen im Datenschutzsinne gar keine legitimationsbedürftige Übermittlung von Patientendaten vor. Vielmehr handelt es sich um eine interne Nutzung durch den verantwortlichen und weisungsbefugten Auftraggeber, die allerdings durch schriftliche Verträge geregelt sein muss. Fehlt es in diesen Fällen schon an der Erforderlichkeit einer Einwilligung, kommt bei einer Zustimmungsversagung erst recht keine Behandlungsverweigerung in Betracht.

Dieser Konflikt zwischen einem immer stärker auf Effizienz und Standardisierung orientierten Gesundheitswesen einerseits und individuellen Patientenrechten und Arztpflichten andererseits wird weiter an Bedeutung gewinnen. Wir haben uns zu der Problematik deswegen auch mit Beiträgen in Fachzeitschriften geäußert.

9.7 Verbindliche Einladungen zu Früherkennungsuntersuchungen von Kindern

Das komplexe Einladungs- und Meldeverfahren für die Früherkennungsuntersuchungen U6 und U7 haben wir auch in der Umsetzung weiter begleitet und datenschutzrechtlich verbessert.

Im 22.TB (9.5) hatten wir von unserer Teilnahme an einer Anhörung des zuständigen Bürgerschaftsausschusses zum Gesetzgebungsvorhaben „Verbindliches Einladungswesen für Früherkennungsuntersuchungen“ berichtet. Nach Verabschiedung der Änderungen des Gesundheitsdienstgesetzes, der Meldedatenübermittlungsverordnung und des Hamburger Kinderbetreuungsgesetzes am 15. Dezember 2009 hatten wir uns mit deren Umsetzung zu befassen. Ein Verwaltungsabkommen mit Schleswig-Holstein regelt die Zusammenarbeit mit der Zentralstelle in Neumünster. Handlungsempfehlende Leitlinien strukturieren das Verfahren zwischen

der Zentralstelle und den Bezirksämtern und zwischen den Jugend- und den Gesundheitsämtern.

Gegenstände unserer Beratung waren die Erfassung der Daten in einer Datenbank, Fragen der Anonymisierung oder Pseudonymisierung nach Fallabschluss sowie die strenge Beachtung der unterschiedlichen Aufgaben von Jugendämtern und Gesundheitsämtern. Bei der Datenerfassung haben wir uns gegen Freitextfelder gewandt, in denen individuelle Gründe für eine Nichtteilnahme an einer U6 / U7-Untersuchung dokumentiert werden können. Wir haben ferner erreicht, dass die Zentralstelle nicht schon unzustellbare Einladungen oder Erinnerungen an das Jugendamt weitergibt und dass eine Pflicht zur Vorlage des Mutterpasses entfällt.

Nachvollziehen konnten wir das Bedürfnis, bei später publik werdenden gravierenden Kindeswohlgefährdungen auch nach dem konkreten Fallabschluss noch auf die Verfahrensdaten zurückgreifen zu können. Dies erschien uns jedoch nur über eine sichere Pseudonymisierung mit einer Schlüsselliste vertretbar, die bei einer leitenden Person extern verwahrt wird.

Zu klären war auch die grenzüberschreitende Kommunikation bei Zu- und Wegzügen während der Einladungsfristen. § 7a Gesundheitsdienstgesetz spricht von einer Übermittlung an das „für den Wohnsitz der gesetzlichen Vertreterin oder des gesetzlichen Vertreters zuständige Fachamt Jugend- und Familienhilfe“. Wir halten es deswegen für zulässig, dass die Zentralstelle versäumte Früherkennungs-Untersuchungen grundsätzlich auch an außerhamburgische Jugendämter übermittelt.

Inzwischen wurde das Modellprojekt durch Gesetz um ein Jahr verlängert. Beratungsbedarf sehen wir vor allem zur Fortführung des Datenbankverfahrens in den Bezirken und zur begleitenden wissenschaftlichen Evaluation des gesamten Projekts.

9.8 Orientierungshilfe Krankenhausinformationssysteme

Unsere Bemühungen um mehr Datenschutz bei elektronischen Patientendatenverwaltungssystemen mündeten in eine bundesweite Orientierungshilfe, die zu einen intensiven Dialog mit Krankenhausträgern und Software-Herstellern führte.

Im 22.TB (9.1) berichteten wir, dass unser 40-Punkte-Katalog „Normative Eckpunkte für Zugriffe auf elektronische Patientendaten im Krankenhaus“ 2009 von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder aufgegriffen und zur Weiterentwicklung an eine Bund-Länder-Arbeitsgruppe überwiesen wurde. Unter Vorsitz des Berliner Datenschutzbeauftragten erarbeitete diese Arbeitsgruppe auf der Grundlage unserer

Eckpunkte und mit unserer Beteiligung ein Dokument, das neben den normativen Vorgaben für die Zugriffsberechtigungskonzepte der Krankenhäuser auch umfangreiche „Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen“ formulierte. In zwei Anhörungen wurden Experten der Krankenhausträger, Wissenschaftler und Software-Hersteller zu den Entwürfen befragt. Im Februar 2011 stellte die Arbeitsgruppe die insgesamt 44 Seiten starke „Orientierungshilfe“ fertig. Mit der Deutschen Krankenhausgesellschaft diskutierte die Arbeitsgruppe gesondert Details der Regelungen.

Sowohl die Konferenz der Datenschutzbeauftragten als auch der „Düsseldorfer Kreis“ – die Bundes-Konferenz der Datenschutz-Aufsichtsbehörden für den nicht öffentlichen Bereich – nahmen das Dokument als künftigen Maßstab für die datenschutzrechtlichen Prüfungen von Krankenhausinformationssystemen an.

Nach diesen Beschlüssen haben wir den Geschäftsführungen aller Hamburger Krankenhäuser die Orientierungshilfe mit der Bitte zur Verfügung gestellt, die jeweiligen Krankenhausinformationssysteme auf ihre Übereinstimmung mit der Orientierungshilfe hin zu überprüfen. Im November 2011 stellten wir das Dokument noch einmal in einer Veranstaltung der Hamburger Krankenhausgesellschaft vor und erörterten Anmerkungen und Kritik der dort ebenfalls referierenden Experten der Deutschen Krankenhausgesellschaft.

Die Orientierungshilfe wird von allen Seiten als die erste bundesweit einheitliche und auf den Klinikalltag bezogene Konkretisierung der datenschutzrechtlichen Anforderungen gelobt und hat sowohl bei den Krankenhausträgern als auch bei den Herstellern eine rege Diskussion zum Patientendatenschutz ausgelöst. Ein inhaltlicher Dissens zwischen den Datenschutzbehörden und den Krankenhausträgern ist noch festzustellen zur Frage, ob und unter welchen Voraussetzungen Patientendaten innerhalb eines Krankenhauskonzerns ausgetauscht werden dürfen und ob ein Krankenhaus ohne ausdrücklichen Widerspruch des Patienten alle früheren Behandlungsdaten auch anderer Einrichtungen eines gemeinsamen Konzerns heranziehen darf. Auch zum Umfang der Protokollierung der Datenzugriffe durch die Krankenhausmitarbeiterinnen und -mitarbeiter und zur Auswertung der Protokolldaten bestehen noch unterschiedliche Vorstellungen. Wir haben deutlich gemacht, dass die Orientierungshilfe eine wertvolle Richtschnur für die Beurteilung der zu prüfenden Krankenhausinformationssysteme darstellt, dass wir jedoch in jedem Einzelfall die datenschutzrechtlichen Vorgaben mit den Argumenten der Kliniken und Krankenhausträger abwägen. Dies verlangt schon das Gebot der Verhältnismäßigkeit. Mit dem UKE sind wir dazu in einem kontinuierlichen Austauschprozess (s.o. 9.1.1 bis 9.1.3).

10. Forschung

10.1 Datenschutzrechtliche Beratung medizinischer Forschungsprojekte

Der Beratungsaufwand für medizinische Forschungsprojekte des UKE hat deutlich zugenommen. Neben Biomaterialbanken waren Register und Online-Befragungen neue Schwerpunkte.

Im Berichtszeitraum haben wir 50 Forschungsprojekte datenschutzrechtlich geprüft und beraten. Die meisten wurden naturgemäß aus dem UKE an uns herangetragen, 10 Forschungsprojekte erreichten uns aus Behörden, Instituten außerhalb des UKE und anderen Krankenhäusern.

Vielfach fordert die Ethik-Kommission der Ärztekammer von den antragstellenden Wissenschaftlern, dass sie auch das Votum des Hamburgischen Datenschutzbeauftragten einholen. In Ihrer Stellungnahme weist die Ethik-Kommission aber auch schon selbst auf datenschutzrechtliche Defizite oder Unklarheiten hin. Sie entwickelte in Abstimmung mit uns auch eine allgemeine Datenschutzklausel für eine pseudonyme oder anonyme Probandendatenverarbeitung.

Die nach der Stellungnahme der Ethik-Kommission von uns erbetene Beratung ist dann regelmäßig zeitkritisch, damit die vorgesehenen Zeitabläufe nicht in Gefahr geraten. Wir fordern von den Forschern zumindest eine Projektbeschreibung (meist den Antrag für die Ethik-Kommission), die Aufklärung der potentiellen Probanden und die Einwilligungserklärung sowie ggf. das Votum der Ethik-Kommission an. Besonders bei nationalen oder internationalen Kooperationsprojekten können die Verfahren des Datenaustausches komplex sein.

Mit den zunehmenden Analysemöglichkeiten mehren sich auch die Projekte zum Aufbau von Probenbanken, vgl. z. B. unten 10.2. Hier ist datenschutzrechtlich vor allem die Pseudonymisierung der Proben und Daten und ggf. die Zusammenführung verschiedener in Zeitintervallen gewonnener Informationen zu demselben Probanden zu prüfen. Immer geht es auch darum, für die Probandenaufklärung und die Einwilligung einen Mittelweg zwischen dem für die Willensbildung optimalen Umfang einerseits und der Verständlichkeit und Nachvollziehbarkeit der Informationen für den Probanden andererseits zu finden. Besonders bei Projekten, bei denen auch Minderjährige als einwilligungsfähige Probanden in Betracht kommen, ist dies eine Herausforderung.

Mehrfach hatten wir es im Berichtszeitraum mit Projekten zu tun, die den Aufbau eines überregionalen Registers – z. B. für spezifische seltene

Erkrankungen – zum Gegenstand hatten. Auch hier musste sichergestellt werden, dass die beteiligten Krankenhäuser ausschließlich anonyme oder pseudonyme Daten an die Registerzentrale melden, die diese an externe Forscher weitergibt. Gerade bei den wenig erforschten Krankheiten liegt zum Zwecke einer Langzeitbetrachtung eine Datenspeicherung ohne zeitliche Befristung nahe. Dies würde jedoch zu sehr unklaren Situationen in der Zukunft führen und angesichts der immer weiter zunehmenden genetischen Analyse- und Vergleichsmöglichkeiten langfristig auch das Re-Identifikationsrisiko erhöhen. Eine 30-jährige Speicherung der pseudonymen Daten in dem Register haben wir dagegen akzeptiert, weil eine Erforschung seltener Krankheiten die erst in vielen Jahren messbaren Auswirkungen von neuen therapeutischen Ansätzen umfasst. Gerade bei sehr langfristigen Registern sollte jedoch auch die Schaffung einer eigenen Rechtsgrundlage – wie etwa bei den Krebsregistern – erwogen werden.

In jüngster Zeit wurden uns auch mehrere Online-Befragungen zur Stellungnahme vorgelegt. Dabei geht es darum, dass die Probanden über einen mitgeteilten Internet-Link auf einen Fragebogen zugreifen und ihn anonym ausfüllen. Hier werden regelmäßig eine spezielle Software und ein speziell gesicherter Server eines Auftragnehmers in Anspruch genommen, wobei z. B. die Speicherung der IP-Nummer ausgeschlossen wird. Problematisch wird es jedoch, wenn zu einem späteren Zeitpunkt eine weitere pseudonyme Datenerhebung erfolgen und der Proband per E-Mail daran erinnert werden soll. E-Mail-Adressen werden sowohl beim Arbeitgeber / Dienstherrn als auch privat zumeist aus dem Vor- und Nachnamen gebildet. Deswegen kann eine Pseudonymität oder Anonymität der Umfrage-Angaben nur dann aufrechterhalten werden, wenn auf jede (technische) Verbindung zwischen der Erinnerung und dem nachfolgenden Ausfüllen des Fragebogens vollständig verzichtet wird. Entweder sollte auf eine direkte Ansprache des Probanden ganz verzichtet werden, oder aber er ist bei der Abfrage der E-Mail-Adresse über deren Verwendung und ihre Risiken ausreichend aufzuklären.

10.2 Biomaterialbank der Martiniklinik des UKE

Beim Aufbau einer Biomaterialbank zur Erforschung von Prostatatumoren haben wir eng und konstruktiv mit der Martiniklinik zusammengearbeitet.

Ende 2010 bat uns die Martiniklinik am UKE GmbH um die datenschutzrechtliche Überprüfung einer geplanten Biomaterialbank. Hierbei ging es vor allem um die Trennung von Behandlungsdaten einerseits und Forschungsdaten und –proben andererseits sowie um die Vernetzung der verschiedenen Datenquellen und die Pseudonymisierung.

Ausgangspunkt ist die Krankenakte des Patienten, die bei der Aufnahme in der Martiniklinik eingerichtet wird. Sie enthält Anamnesefragebogen, Behandlungsdokumentation und später Follow-up- Fragebogen und wird in der elektronischen Datei „Martini-Data“ geführt. Zugang zu dieser Datei hat ausschließlich das Behandlungsteam der Martiniklinik. Nur Begleiterkrankungen und Medikation werden auch in der Soarian-Akte des UKE erfasst. Bereits bei der Aufnahme werden den Patientendatensätzen – nach Einholung einer Einwilligung – ein erstes Pseudonym („Biobank-Nr.“) hinzugefügt und Etiketten mit dieser Code-Nummer gedruckt. Bei den Untersuchungen und während der OP werden Gewebe-, Blut-, Urin-, Sekretproben entnommen und teilweise an das Pathologische Institut des UKE zur Diagnostik versandt und teilweise für den Aufbau einer Biomaterialbank der Martiniklinik verwandt. Diese letztgenannten Proben werden mit den Code-Etiketten versehen, ins Labor gebracht, registriert und dann eingefroren.

Forschende wenden sich mit ihren spezifischen Fragestellungen an den Leitenden Arzt der Martiniklinik, der aus „Martini-Data“ eine entsprechende Liste von Patienten mit den relevanten Daten, einschließlich der Befunde durch das Pathologische Institut, zusammenstellt. Anhand der Biobank-Nummern sucht das Personal des Labors die entsprechenden Proben heraus und zweigt davon die notwendige Teilmenge für die forschende Person ab. Ein Datentreuhänder pseudonymisiert die Biobank-Nummer wiederum durch einen Studiencode, mit dem das Labor die Teilprobe kennzeichnet und dem Forscher zur Verfügung stellt. Nur der Datentreuhänder verwahrt die 2. Schlüsselliste (Biobank-Nr. / Studiennummer). Spätere Follow-up-Daten werden über nachträgliche schriftliche Befragungen der Patienten in „Martini-Data“ erfasst und z. B. für Verlaufs-Studien über eine kurzzeitige Re-Identifikation durch den Datentreuhänder dem Forscher pseudonym zur Verfügung gestellt.

Dieses Verfahren wird in der Anweisung (SOP) 7.4.2 der Martiniklinik ausführlich beschrieben, dem Patienten in einer umfangreichen Aufklärung erläutert und erst nach der schriftlichen Einwilligung umgesetzt. Durch ein entsprechendes Einwilligungs-Häkchen in Martini-Data wird sichergestellt, dass ohne eine Einwilligung keine Probe in die Biomaterialbank aufgenommen wird. Die Aufklärung enthält auch den Hinweis auf die Freiwilligkeit und Widerruflichkeit der Einwilligung und die Folgen eines Widerrufs. In einem Prüfungstermin vor Ort haben wir uns von der Umsetzung der vereinbarten Prozeduren und technisch-organisatorischen Sicherungsmaßnahmen überzeugt. Nicht näher eingegangen sind wir auf die „Schnittstelle“ zur Soarian-Akte des UKE, da dies das oben in 9.1 beschriebene

allgemeine Problem der Konzernstruktur und „Mandantenorientierung" von SOARIAN betrifft.

11. Hochschulwesen

11.1 Teilnahme am dialogorientierten Serviceverfahren Hochschulzulassung

Die Teilnahme Hamburgischer Hochschulen am Serviceverfahren der Stiftung Hochschulzulassung muss datenschutzgerecht erfolgen, bedarf nach unseren Feststellungen aber keiner gemeinsamen Datei von Stiftung und Hochschulen.

Durch den Staatsvertrag über die Errichtung einer gemeinsamen Einrichtung für Hochschulzulassung vom 11.11.2008, der in Hamburg mit Gesetz vom 25.05.2010 umgesetzt worden ist, sollte das Hochschulzulassungswesen in zulassungsbeschränkten Studiengängen neu geordnet werden. Neben wenigen Studiengängen, die weiterhin einer zentralen Studienplatzvergabe durch die Stiftung Hochschulzulassung mit Sitz in Nordrhein-Westfalen vorbehalten sind, sollte den Hochschulen durch ein sogenanntes Serviceverfahren die Möglichkeit eröffnet werden, sich freiwillig an einem bundesweiten Clearingverfahren zu beteiligen, das ihnen jedoch die Zulassungsentscheidung belässt.

Die Vergangenheit hatte gezeigt, dass die Zulassung zu zugangsbeschränkten Studiengängen, die ausschließlich durch die einzelnen Hochschulen vorgenommen wurde, aufgrund der oft mehrfach durchzuführenden Nachrückverfahren zu dem unbefriedigenden Ergebnis geführt hatte, dass Studienanfänger ihr Studium erst mit erheblichen Verzögerungen aufnehmen konnten oder Studienplätze ganz unbesetzt blieben. Dem konnte bei bloß freiwilliger Teilnahme der Hochschulen nicht wirksam begegnet werden. Die Kultusministerkonferenz hat deshalb schließlich eine obligatorische Anbindung an das Serviceverfahren beschlossen.

Anders als in anderen Ländern wird die Hochschulzulassung in Hamburg bisher per Satzung durch die einzelnen Hochschulen geregelt. Für eine verpflichtende und datenschutzgerechte Teilnahme am Serviceverfahren bedurfte es daher kurzfristig einer Änderung des Umsetzungsgesetzes, um noch zum Sommersemester 2012 ab 01.04.2012 am Verfahren teilnehmen zu können.

Die Einzelheiten des Verfahrens, u. a. eine Musterrechtsverordnung und die technische Umsetzung waren von der Stiftung bis dahin ausschließlich nach nordrhein-westfälischem Recht betrachtet worden, wobei spätestens durch die verpflichtende Teilnahme der Hochschulen datenschutzrechtlich

nicht mehr von einer Auftragsdatenverarbeitung ausgegangen werden konnte, sondern Regelungen für eine länderübergreifende gemeinsame Datenverarbeitung mit den erforderlichen Regelungen zu den einzelnen Verantwortlichkeiten erforderlich erschienen. Dies ist noch umzusetzen.

Auch das erst im September 2010 zur Verfügung gestellte und im Oktober mit der Stiftung länderübergreifend diskutierte Datenschutzkonzept hatte diese Änderung der rechtlichen Grundlagen noch nicht berücksichtigt. Es hat den Eindruck einer gemeinsamen Datei vermittelt, woran jedoch nach den mündlichen Ausführungen deutliche Zweifel aufgekommen sind.

In Anbetracht dessen, dass in Hamburg nicht nur eine Verordnung, sondern zuvor noch die gesetzliche Grundlage für eine zentrale Verordnung geschaffen werden muss, haben wir daher kurzfristig mit der für das Verfahren verantwortlichen Stiftung zu klären versucht, in welchem Umfang eine gemeinsame Datenverarbeitung oder Zugriffe im Abrufverfahren erforderlich sind. Dabei ist letztlich herausgekommen, dass eine gemeinsame Datei weder mit der Stiftung noch mit anderen Hochschulen erforderlich ist. Das von der Stiftung vorgesehene Verfahren sieht lediglich vor, dass die Hochschulen bei der Stiftung die sie betreffenden Daten der Bewerber abrufen können. Die Bezeichnung als dialogorientiertes Verfahren sollte sich dem Vernehmen nach auch mehr auf den Kontakt mit den Studierenden beziehen, die sich auf der zentral von der Stiftung zur Verfügung gestellten Plattform bewerben können.

Einer Ermächtigung zum Führen einer gemeinsamen Datei nach § 11 a des Hamburgischen Datenschutzgesetzes (HmbDSG) hätte es nach unserer Auffassung somit nicht bedurft. Wir hatten daher empfohlen, auf die Rechtsänderung zu verzichten. In Anbetracht des schwierigen bundesweiten Klärungsprozesses und der engen zeitlichen Vorgaben für den Landesgesetzgeber haben wir uns schließlich bereit erklärt, unsere Bedenken gegen die vorgeschlagene Regelung zurückzustellen, wenn sichergestellt ist, dass die Ermächtigung bei nächster Gelegenheit zurückgenommen wird, soweit sie sich bei der Umsetzung als nicht erforderlich erweist.

11.2 Hochschulübergreifendes Identitätsmanagementsystem eCampus-IDMS

Nach der Änderung des Hamburgischen Hochschulgesetzes kommt es nun auf die Schaffung einer normenklaren und datenschutzgerechten Mustersatzung an, die die Verarbeitungsbefugnisse und Verantwortlichkeiten datenschutzkonform regelt.

Das Projekt Hochschulübergreifendes Identitätsmanagementsystem (eCampus-IDMS) haben wir bereits im letzten Tätigkeitsbericht (22.TB,

11.1) ausführlich behandelt. Ziel des Projekts ist es u. a., alle an Hamburger Hochschulen Studierende und sonstige Mitglieder unter jeweils nur einer Kennung zu führen, egal an wie vielen Hochschulen und in welchen Funktionen sie geführt werden.

Mittlerweile ist mit unserer Beteiligung die erforderliche Ermächtigung zur Datenverarbeitung mit dem Zehnten Gesetz zur Änderung des Hamburgischen Hochschulgesetzes (HmbHG) geschaffen worden. Nach § 111 Absatz 4 HmbHG dürfen die Hochschulen und die Staats- und Universitätsbibliothek (Stabi) eine gemeinsame Datei führen, um das eCampus-IDMS betreiben zu können. Nach Absätzen 5 und 6 soll das Nähere durch Hochschulsatzungen bzw. für die Stabi durch Rechtsverordnung des Senats geregelt werden.

Für eine angekündigte Mustersatzung hatten wir unsere Beratung angeboten.

Das multimedia kontor Hamburg (mmkh) hat uns einen ersten Entwurf zukommen lassen, den wir kommentiert und mit dem mmkh erörtert haben.

Neben verschiedenen rechtsdogmatischen Hinweisen zur Abgrenzung von gemeinsamer Datei, Abrufverfahren und Einwilligungslösung ist es uns dabei im Wesentlichen auf folgende Punkte angekommen:

Jede einzelne Satzung bzw. die Rechtsverordnung kann nur ihren eigenen Beitritt zum System und die jeweils gleichlautenden Verarbeitungsbedingungen regeln.

Entsprechend der gesetzlichen Ermächtigung ist der Regelungsgegenstand auf das eCampus-IDMS zu beschränken. Dabei müssen der Zweck und die Verarbeitungsbefugnisse und -grenzen normenklar beschrieben werden.

Wie schon im Rahmen des Projekts hat die Schwierigkeit darin bestanden, den kaskadierenden Ansatz ausreichend zu beschreiben. Danach dürfen nur die wenigen, für die Zwecke des eCampus-IDMS erforderlichen Daten in einem Meta Directory vorgehalten und laufend konsolidiert werden, und alle anderen Daten, insbesondere die Verwaltung der Zugriffsbefugnisse zu den einzelnen Anwendungen und die Anwendungen selbst, müssen bei den jeweiligen Hochschulen vorgehalten und verarbeitet werden.

Wir werden die rechtlichen Regelungen und die Umsetzung des Projekts im Sinne einer datensparsamen und datenschutzkonformen Lösung weiter begleiten.

12. Bauen, Wohnen, Umwelt

12.1 Das Verfahren zur Ermittlung der neuen Sielbenutzungsgebühr

Die Vorbereitung und Umsetzung der neuen Sielbenutzungsgebühr für Regenwasser setzte die Verarbeitung von Bürgerdaten voraus. Wir haben die Hamburger Stadtentwässerung (HSE) dabei datenschutzrechtlich beraten und an der Schaffung der erforderlichen Rechtsgrundlagen mitgewirkt.

In Verlauf der Umstellung der Sielbenutzungsgebühren auf einen neuen Maßstab haben wir viele Eingaben von Bürgerinnen und Bürgern erhalten, die sich unter anderem über die Nutzung von Luftbildern ihres Grundstücks beschwerten.

Ziel der Gebührenumstellung war eine Trennung und verursachergerechte Zuordnung der Gebühren für Schmutzwasser (Maßstab: Frischwasser) einerseits und Regenwasser (Maßstab: versiegelte Fläche) andererseits. Zur Vorbereitung der neuen Regenwassergebühr erfasste die HSE zunächst die gesamte Landesfläche, um den Versiegelungsgrad der Grundstücke zu ermitteln. Dies war insbesondere für Modellrechnungen erforderlich.

Dafür nutzte die HSE die Daten aus dem Liegenschaftskataster sowie Luftbilder aus den Jahren 2007 und 2008. Nach § 13 Abs.4 Satz 2 des Hamburgischen Vermessungsgesetzes (VermG) sind neben einigen Behörden auch die Unternehmen für die öffentliche Abwasserentsorgung (HSE) berechtigt, personenbezogene Grundstücksdaten aus dem Liegenschaftskataster auch ohne eine Interessensabwägung mit den schutzwürdigen Belangen der betroffenen Eigentümer zu erhalten. Einer Anonymisierung der Daten bedurfte es deswegen nicht.

Die amtlichen Luftbilder sind einerseits Geobasisdaten, die jedermann zugänglich gemacht werden können, „soweit öffentliche und private Belange nicht entgegenstehen“, § 10 Abs.4 VermG. Sie können aber – nach Umwandlung in digitalisierte und standardisierte sog. „Orthofotos“ – möglicherweise auch als „anderes flächenbezogenes Fachinformationssystem“ zur Bestimmung des Versiegelungsgrades angesehen werden, das der Führung des Liegenschaftskatasters zum Zweck der Bereitstellung von Geobasisdaten dient, § 11 Abs.3 Nr.6 in Verbindung mit § 1 Abs.1 VermG. Damit können grundstücksbeziehbare Luftbilder grundsätzlich auch Teil des Liegenschaftskatasters werden. Das Landesamt für Geoinformationen als Vermessungsbehörde durfte der HSE deswegen auch die amtlichen Luftbilder zur Vorbereitung der neuen Gebührenregelung zur Verfügung stellen.

HSE nahm für die Auswertung der Daten einen Dienstleister in Anspruch. Dazu haben wir der HSE die datenschutzrechtlichen Anforderungen an die Auftragsdatenverarbeitung benannt und Einfluss auf die Vertragsgestaltung genommen.

Zur Klarstellung, dass die HSE die übermittelten personenbezogenen Daten des Liegenschaftskatasters und amtliche Luftbilder auch entgegennehmen und – auch durch Dritte – verarbeiten darf, wurde Ende 2010 § 13a in das Hamburgische Sielabgabengesetz (SAG) eingefügt. Unsere Anregung zum Gesetzestext wurde übernommen.

Luftaufnahmen lassen allerdings nicht erkennen, ob und in welchem Ausmaß die Grundstückseigentümer das Regenwasser auf dem Grundstück versickern lassen oder aber – und nur das ist zukünftig gebührenrelevant – in das öffentliche Abwassersiel leiten. Hierfür bedurfte es einer Befragung der Hamburger Grundstückseigentümer. Wie wir früh deutlich machten, war dafür eine neue gesetzliche Grundlage erforderlich. § 26 SAG wurde deswegen um eine Vorschrift ergänzt, welche die Grundstückseigentümer zur Auskunft darüber verpflichtet, von welchen Grundstücksflächen (Lage, Art und Größe) Niederschlagswasser in das Abwassersiel eingeleitet wird. Gibt der Eigentümer keine Auskunft, darf die HSE die Flächen anhand der Katasterunterlagen schätzen und als Gebührenbemessungsgrundlage heranziehen. Eigentümer, die das Niederschlagswasser vollständig auf ihrem Grundstück versickern lassen, trifft diese Pflicht zur Auskunft und Rücksendung des Erhebungsbogens nach der Gesetzesformulierung eigentlich nicht. In der Praxis – so die nachvollziehbare Entgegnung der HSE – wird aber jeder Grundstückseigentümer schon im Eigeninteresse die für ihn günstige Auskunft geben wollen, um einer Heranziehung nach Schätzung zu entgehen.

12.2 Geodaten

In einer gemeinsamen Arbeitsgruppe mit der Behörde für Stadtentwicklung und Umwelt (BSU) sowie dem Landesbetrieb für Geoinformationen und Vermessungswesen (LGV) haben wir die Karten-, Bild- und Datei-Angebote des LGV datenschutzrechtlich bewertet und uns in einer Bund-Länder-Arbeitsgruppe für eine praktikable Abgrenzung zwischen datenschutzrechtlich zulässigen und unzulässigen Offenbarungen von Geodaten eingesetzt.

Der LGV bietet die verschiedensten Geodaten in Form von Datensätzen, digitalen Karten und Orthofotos (digitalisierte und standardisierte Luftbilder) auf vielfältigen Vertriebswegen an – zum Teil offline gegen Bezahlung, zum Teil auf Portalen des Intranets der Verwaltung und zum Teil für jedermann über Internetportale. Über die Frage, welche der übermittelten Infor-

mationen personenbeziehbar sind und damit dem Datenschutz unterliegen, wird unter den Datenschutzaufsichtsbehörden seit langem diskutiert. Eine einheitliche Auffassung hat sich bisher nicht gebildet, weil einerseits jede georeferenzierte Information letztlich einem Flurstück, Grundstück und einer Adresse und damit dem Eigentümer zugeordnet werden kann, andererseits aber der Datenschutz den großen Nutzen von Geobasis- und Infrastrukturdaten und den gesetzlichen Auftrag zu ihrem Ausbau nicht konterkarieren soll.

In einer gemeinsamen Arbeitsgruppe mit der BSU und dem LGV haben wir uns über die Produkte und Vertriebswege des LGV unterrichten lassen, datenschutzrechtliche Aspekte eingebracht und Rechtsgrundlagen für die Offenbarung der Geodaten geprüft. So enthält das Hamburgische Vermessungsgesetz (VermG) abgestufte Übermittlungsbefugnisse für Geobasisdaten und Daten aus dem Liegenschaftskataster. Bei einem direkten Personenbezug dürfen Katasterdaten (Eigentümerdaten im Liegenschaftsbuch) nur nach Darlegung eines besonderen berechtigten Interesses des Empfängers im Einzelfall übermittelt werden. Geobasisdaten, zu denen z. B. Luftbilder gehören, dürfen dagegen übermittelt und veröffentlicht werden, „soweit keine öffentlichen oder privaten Belange entgegenstehen“, § 10 Abs. 3 VermG. Für die geplante automatisierte Übermittlung personenbeziehbarer Daten aus dem Baulastenverzeichnis fehlt eine Rechtsgrundlage dagegen ganz, weil § 79 Hamburger Bauordnung nur die Einsichtnahme und einen Ausdruck im Einzelfall zulässt.

Ab welcher Bildschärfe einer Übermittlung von Luftbildern bzw. Orthofotos aus Datenschutzgründen „private Belange“ im Sinne des § 10 Abs.3 VermG entgegenstehen, ist nach wie vor nicht eindeutig geklärt. In Hamburg wie in anderen Bundesländern werden aus Luftbildern digitale Orthophotos (DOP) mit einer Pixelgröße von 10x10 cm (DOP 10) hergestellt und vertrieben. Unter den Datenschutzbeauftragten ist dagegen bislang nur unstrittig, dass ab einer Pixelgröße von 40 cm von der Zulässigkeit einer allgemeinen Veröffentlichung ausgegangen werden kann. Anhand von Foto-Beispielen haben wir uns allerdings davon überzeugt, dass auch bei DOP 10 weder Personen zu identifizieren noch Kfz-Nummern zu erkennen sind. Allerdings können bei DOP 10 Gegenstände im Garten, auf der Terrasse, Autos auf dem Stellplatz deutlicher wahrgenommen (in seltenen Fällen auch überhaupt erst als solche erkannt werden) als bei DOP 40. Aus einer Abwägung des Interesses der (Einfamilienhaus-)Besitzer am Schutz des Besitztums vor fremden Blicken einerseits und dem Bedürfnis nach qualitativ hochwertigen Übersichtsaufnahmen und Infrastrukturdaten andererseits haben wir der Bund-Länder-Arbeitsgruppe der Datenschutzaufsichtsbehörden einen Kompromiss vorgeschlagen. Ohne datenschutzrechtliche

Einzelprüfung sollte ab DOP 20 von der Zulässigkeit einer allgemeinen (Internet-)Veröffentlichung ausgegangen werden. Datenschutzaufsichtsbehörden aus anderen Bundesländern haben sich dem angeschlossen, andere blieben beim DOP 40-Standard. Als Kompromiss wird eine Regel-Zulässigkeit von DOP 20-Veröffentlichungen mit der Möglichkeit, im Ausnahmefall besondere Betroffenen-Belange zu berücksichtigen, diskutiert. Eine Ausnahme könnte z. B. vorliegen, wenn auf dem Luftbild ein Krankenbett mit Patient im Garten deutlich zu erkennen ist.

Der LGV betreibt darüber hinaus einen sog. Fachdatenserver, in den andere Behörden ihre punkt- und flächenbezogenen Fachdaten mit einer „Datenfreigabe-Erklärung“ einstellen, um sie über spezielle Dienste des LGV Verwaltungsstellen und Dritten zugänglich zu machen. Ob durch solche Abrufe und Daten-Verschneidungen mit anderen georeferenzierten Informationen datenschutzrechtlich problematische Informationen entstehen, liegt in der Verantwortung der abrufenden Stelle, nicht des LGV oder der bereitstellenden Behörden.

Da es hier jeweils auf die zusammengeführten Datenarten ankommt, ist eine Einzelfallprüfung nicht zu vermeiden. Unproblematisch sind Informationen, die auf mehr als drei Grundstücke bezogen (aggregiert) sind und nicht auf alle zutreffen. Ohne eine solche Aggregierung sehen wir topografische Boden- und Umweltdaten auch als Punktdaten grundsätzlich für weniger schutzbedürftig an als Informationen, die auf Entscheidungen bzw. Verhalten oder Eigenschaften der Grundstückseigentümer zurückgehen wie z. B. Zimmer-Anzahl, Energieeffizienzdaten, Baukosten usw. Risikodaten, die den Wert des Grundstückes entscheidend beeinflussen, wie Altlasten oder ein Munitionsverdacht, sind dagegen auch datenschutzrechtlich sensibel. Dagegen sollten Grundstücksdaten, die auch durch DOP 20 erkennbar sind, wie Größe und Lage eines Teiches oder eines Schuppens im Garten, frei verfügbar sein.

13. Wahlen und Volksabstimmungen

13.1 Nochmals: Vordrucke für Briefwahlunterlagen

Die seit 2007 erörterten Datenschutzdefizite bei den Vordrucken für Briefwahlunterlagen sind auch bei den vorgezogenen Neuwahlen zur Hamburgischen Bürgerschaft 2011 zu bemängeln gewesen.

Zur Problematik frei einsehbarer Briefwahlanträge hatten wir ausführlich im letzten Tätigkeitsbericht berichtet (III 13.1): Antragsformulare im Postkartenformat mit Adressvordruck verleiten unnötig zur Preisgabe von Namen, Adresse, Geburtsdatum und Unterschrift an jedermann, auch

wenn im allgemeinen Anschreiben auf die datenschutzgerechtere Möglichkeit der Versendung im Briefumschlag hingewiesen wird. Wir halten eine Umgestaltung der Vordrucke für eine angemessene organisatorische Datenschutzmaßnahme, zumal andere Länder dies auch ohne ausdrückliche Regelung praktizieren und das Bundeswahlrecht die Gestaltung des Antrags abschließend in DinA-4-Format vorschreibt mit zusätzlichem Hinweis auf verschlossene Versendung. Hierüber waren wir mit dem Landeswahlamt seit 2007 mehrfach im Gespräch.

Es hat uns daher überrascht, als auch 2011 zur vorgezogenen Neuwahl wieder Beschwerden eingegangen sind über die monierte Ausgestaltung des Vordrucks.

Hierzu hat uns das Landeswahlamt mitgeteilt, dass man wegen der Eile der Vorbereitungen auf die bei der letzten Bundestagswahl eingesetzte Benachrichtigung zurückgegriffen habe. Wie im letzten Bericht dargelegt, hat auch diese schon den bundesgesetzlichen Anforderungen nicht genügt.

Das Landeswahlamt hat uns nun bestätigt, dass unverändert eine datenschutzfreundlichere Ausgestaltung vorgesehen sei und wir dazu einbezogen würden.

Der Freien und Hansestadt Hamburg sollte der Schutz der personenbezogenen Daten seiner Bürgerschaftswahlberechtigten nicht weniger wert sein als anderen Bundesländern und Vorrang haben vor etwaigen fiskalischen Überlegungen.

13.2 Videokameras in Wahllokalen

Auf die Nutzung von Wahllokalen in Bankfilialen, die im normalen Betrieb videoüberwacht werden, sollte verzichtet werden. In sonstigen öffentlichen Gebäuden sollten die Kameras, die das Innere des Wahllokals aufnehmen können, hinreichend deutlich für die Wähler deaktiviert werden. Dabei sollte das Vieraugenprinzip beachtet und die Abschaltung protokolliert werden.

Bereits im Jahre 2004 war die Videoüberwachung in Wahllokalen, insbesondere in Banken, gegenüber dem damaligen Hamburgischen Datenschutzbeauftragten problematisiert worden. Seinerzeit waren eine Abschaltung der Kameras und ein Hinweisschild am Wahllokal mit der Aufschrift „Der Wahlraum wird nicht videoüberwacht“ als ausreichende Maßnahmen mit dem Landeswahlamt vereinbart worden.

Eine neuerliche Eingabe hat uns schließlich zu einer Neubewertung der Risiken bewegt:

Wie uns zugetragen worden ist, werden Bankfilialen nicht nur offen, sondern auch durch nicht ohne weiteres erkennbare Kameras überwacht.

Die fortgeschrittenen technischen Möglichkeiten lassen nicht immer eine Kamera erkennen. Nach der neueren Rechtsprechung des Bundesverfassungsgerichts kann eine Beschwer auch in der verhaltenslenkenden Wirkung einer Videoüberwachung liegen.

Nach diesen Maßstäben begrüßen wir das Bestreben der Wahlleitungen, auf Wahllokale in Bankfilialen ganz zu verzichten.

Soweit andere öffentliche Gebäude genutzt werden, die im normalen Betrieb videoüberwacht werden, wie z. B. Außenanlagen von Schulen, sollten zur Vermeidung verhaltenslenkender Wirkungen alle Kameras, die sich im Wahllokal befinden oder das Innere des Wahllokals von außen mit ihrem Aufnahmewinkel erfassen können, ausgeschaltet und im Rahmen des Zumutbaren zusätzlich abgedeckt werden. Die Abschaltung sollte nach dem Vier-Augen-Prinzip erfolgen und protokolliert werden.

Wir haben mit dem Landeswahlleiter vereinbart, dass wir uns für den Fall, dass ein Rückgriff auf Bankfilialen im Einzelfall nicht vermeidbar ist, an der Erarbeitung eines hinreichenden Datenschutzkonzepts beteiligt würden. Sowohl bei der Volksabstimmung 2010 als auch bei der vorgezogenen Bürgerschaftswahl 2011 brauchte man auf Bankfilialen nicht mehr zurück zu greifen.

13.3 Projekt Wahlunterstützung der Bezirksämter

Auch die mit der Wahlvorbereitung verbundene personenbezogene Datenverarbeitung bedarf rechtlicher Grundlagen. Für eine einheitliche Handhabung bietet sich die Übernahme bundesrechtlicher Vorschriften im Landesrecht an.

Zu den Aufgaben der bezirklichen Wahldienststellen gehört die Sicherstellung der Wahlabläufe am Wahltag, insbesondere also die Bereitstellung von Wahllokalen und Wahlvorständen in ausreichender Zahl einschließlich der anschließenden Auszahlung der Aufwandsentschädigung. Hierfür haben die Bezirke bisher in unterschiedlicher Form auf Daten vorangegangener Wahlen zurückgegriffen.

Im Herbst 2010 ist uns das Projekt Wahlunterstützung der Bezirksämter vorgestellt worden, das als angepasste Standardsoftware für diese Zwecke von allen Bezirken eingesetzt werden sollte und zur planmäßigen Wahl 2012 erstmals zur Verfügung stehen sollte. Nach der vorgezogenen Neuwahl sind uns die maßgeblichen Unterlagen vorgelegt und im Herbst 2011 das Standardprodukt vorgeführt worden.

Wir haben das Projekt frühzeitig beraten. Von datenschutzrechtlichem Interesse sind insbesondere die Führung einer Historie sowie die Verarbei-

tungsbefugnisse für die verschiedenen Formen von Wahlen und Abstimmungen nach Bundes- und Landesrecht gewesen. Daneben haben wir auf die zusätzlichen rechtlichen Anforderungen bei bezirksübergreifender Verarbeitung in einer gemeinsamen Datei hingewiesen, auf die im Laufe des Projekts jedoch verzichtet wurde.

Bereits in früheren Zusammenhängen hatten wir in Ermangelung landesrechtlicher Vorschriften empfohlen, für die dauerhafte Speicherung von Wahlhelferdaten aus Bürgerschaftswahlen die Einwilligung der Betroffenen einzuholen. Grundsätzlich sind zur Durchführung der anstehenden Wahl jedoch mehr personenbezogene Daten erforderlich als für die Neuwerbung für künftige Wahlen. Die Grundsätze der Datensparsamkeit und der Erforderlichkeit sind auch hier zu beachten.

Für die Bundes- und Europawahlen gilt mit § 9 Absatz 4 des Bundeswahlgesetzes (BWahlG) die gesetzliche Regelung, dass für künftige Wahlen nur bestimmte Grunddaten, die Anzahl der Berufungen sowie die dabei ausgeübte Funktion als Historie gespeichert werden dürfen. Angaben über Schulungen, konkrete Einsatzorte und auch die Abrechnungsdaten gehören nicht dazu.

Tatsächlich ist die Verwaltung von Einwilligungslösungen, die jederzeit und in beliebigem Umfang widerrufen werden können, sehr aufwändig. Auch wenn damit mehr Daten für die Historie legitimiert werden könnten, haben wir gleichwohl empfohlen, darauf hinzuwirken, dass in die Hamburgische Wahl- und in die Hamburgische Abstimmungsordnung Regelungen aufgenommen werden, die mit § 9 Absatz 4 BWahlG kompatibel sind.

Damit verbunden ist allerdings ein aufwändigeres Löschungskonzept, das derzeit noch angepasst wird.

Für die notwendige Übernahme der Daten aus den bisherigen Anwendungen haben wir gebeten, durch ein entsprechendes Verfahren sicherzustellen, dass nur Datensätze mit tatsächlich vorliegender schriftlicher Einwilligungserklärung in das neue Verfahren übernommen werden.

14. Verkehr

14.1 Verkehrszählung per Videoüberwachung durch die Hamburg Port Authority

Auch bei Verkehrszählungen haben öffentliche Stellen die Grenzen zu beachten, die das Bundesverfassungsgericht an die Videoaufzeichnung von KFZ-Kennzeichen stellt. Im Wege der Auftragsdatenverarbeitung können keine Leistungen eingekauft werden, die der auftraggebenden Stelle nicht schon von Gesetzes wegen zugewiesen wurden.

Im Sommer 2010 sind wir durch verschiedene Anrufe auf eine Verkehrszählung aufmerksam gemacht worden, die seitens eines renommierten Unternehmens im Auftrag der Hamburg Port Authority (HPA) durchgeführt wurde. Sie sollte der Erfassung der Fahrzeugverkehre im Hafengebiet dienen und die Potenziale von Elektromobilität abschätzen. Dazu war ein Beratervertrag geschlossen worden, der der HPA zwar Weisungsrechte und die Herausgabe der Ergebnisse sicherte, nicht aber den Umgang mit den Rohdaten. Es war vereinbart worden, dass die Datenverarbeitung nach § 4 BDSG erfolgen sollte.

Die Erhebung sollte sechs Tage lang durch Aufzeichnung und spätere automatisierte Pseudonymisierung der KFZ-Daten, durch freiwillige Fahrzeugführerbefragungen und GPS-unterstützte Routenverfolgung erfolgen. Die KFZ-Daten wurden dafür unverschlüsselt auf Filmmaterial in Echtzeit aufgezeichnet und sollten nach Beendigung der Maßnahme in den Räumen der Auftragnehmerin wiederum in Echtzeit pseudonymisiert und verschlüsselt werden.

Vorab war schon zu Testzwecken in entsprechender Weise verfahren und das Material unverschlüsselt ins Archiv der Auftragnehmerin überführt worden.

Für diese Vorgehensweise haben wir weder eine hinreichende rechtliche Grundlage erkennen können noch entsprach der Aufbau des Verfahrens den Anforderungen der Rechtsprechung des Bundesverfassungsgerichts an eine datenschutzgerechte Verarbeitung von KFZ-Kennzeichen durch Videoaufzeichnung. Wir haben die HPA deshalb aufgefordert, die Erhebung sofort einzustellen und die erhobenen Kennzeichen zu löschen, was sie auch umgehend veranlasst hat.

Im Einzelnen haben wir uns von folgenden Überlegungen leiten lassen:

Die Videoüberwachung mit Aufzeichnung stellt für alle Betroffenen grundsätzlich einen erheblichen Eingriff in ihr informationelles Selbstbestimmungsrecht dar und darf nur auf der Grundlage einer hinreichend bestimmten und verhältnismäßigen Rechtsgrundlage erfolgen. Die KFZ-Kennzeichen sind personenbezogene Daten nach § 45 Satz 2 des Straßenverkehrsgesetzes (StVG). Zweck der Erhebung sind Planungs- oder eventuell Forschungszwecke. Auf die HPA als Auftraggeberin finden die Vorschriften des Hamburgischen Datenschutzgesetzes (HmbDSG) Anwendung. Mangels spezialgesetzlicher Regelungen kamen nur die Vorschriften des HmbDSG in Betracht. Sowohl die Verarbeitung zu Planungszwecken als auch die Verarbeitung zu Forschungszwecken scheitern an der Voraussetzung, dass sie im überwiegenden Allgemeininteresse erforderlich sein müssen.

Angesichts der bestehenden und etablierten Verfahren zur unmittelbaren Pseudonymisierung bei Aufzeichnung der Daten haben wir das eingesetzte Verfahren nicht mehr als datenschutzrechtlich erforderlich ansehen können.

Die GPS-gestützte Verfolgung der Betroffenen stellt eine Erhebung personenbezogener Daten ohne Kenntnis der Betroffenen dar, für die die gesetzlichen Anforderungen des § 12 HmbDSG nicht vorlagen. Eine Erweiterung der Befugnisse durch die Beauftragung privater Dritter, denen in eigener Sache weitergehende Verarbeitungsbefugnisse zustehen mögen, ist mit der Beauftragung privater Stellen für öffentliche Stellen nicht verbunden.

Zu beanstanden war auch der Testlauf mit Echtdaten.

Schließlich hätte eine Vorabkontrolle die Risiken und die Unzulässigkeit des Verfahrens rechtzeitig aufdecken können.

Wir haben der HPA im weiteren grundsätzliche Hinweise für eine datenschutzgerechte Ausgestaltung des Verfahrens als Auftraggeberin gegeben. Hierzu gehören auch Hinweise zur sofortigen Pseudonymisierung bei der Aufnahme von Videobildern.

Soweit Personenbeziehbarkeit besteht oder durch Verknüpfung mit weiteren Merkmalen wieder hergestellt werden kann, sind die Anforderungen der Auftragsdatenverarbeitung zu beachten.

Wir haben mangels örtlicher Zuständigkeit nicht weiter vertieft, in welchem Umfang der Auftragnehmerin aus eigenem Forschungsinteresse ein Datenverarbeitungsanspruch zustehen könnte, wenn sie die Daten auf eigenes Risiko erforschen und die Ergebnisse erst anschließend zum Verkauf zur Verfügung stellen würde.

14.2 Modernisierung des Ordnungswidrigkeitenverfahrens

Die derzeit verfolgte teilweise elektronische Aktenführung konnte in der erforderlichen Rechtsverordnung hinreichend abgebildet werden. Eine nicht datenschutzkonforme Verarbeitung im außereuropäischen Ausland konnte im Zusammenwirken mit dem Projekt erfolgreich abgewendet werden.

Bereits im Jahre 2008 war das Projekt „OWI21 für Hamburg“ eingesetzt worden, um das alte Verfahren OPAL zur Unterstützung der Sachbearbeitung von Ordnungswidrigkeitenverfahren im Bereich des Straßenverkehrs abzulösen. Wir hatten in der Vergangenheit einzelne Hinweise gegeben und insbesondere Fragestellungen im Zusammenhang mit den Löschungsfristen gemeinsam erörtert. Im Berichtszeitraum haben wir im Wesentlichen folgende Fragestellungen behandelt:

Einbindung der elektronischen Aktenführung:

Eines der Ziele des Projekts ist die Einbindung der elektronischen Aktenführung, die nach § 110 b des Ordnungswidrigkeitengesetzes (OWiG) grundsätzlich auf der Grundlage einer landesrechtlichen Verordnung zulässig ist. Im Herbst 2010 hat uns hierzu ein Entwurf erreicht, den wir aus datenschutzrechtlicher Sicht ausführlich kommentiert haben. Am 01.04.2011 ist die Verordnung über die elektronische Aktenführung in Bußgeld- und Verwarnungsangelegenheiten in Kraft getreten. Sie regelt die Aktenführung nur sehr allgemein. Wichtig ist uns unter anderem die Beschränkung elektronischer Suchfunktionen auf den Einzelfall und eine kurze, dem Tatvorwurf und dem Verfahrensablauf angemessene Aufbewahrungsfrist gewesen. Um eine funktionierende rechtsverbindliche elektronische Dokumentation zu gewährleisten, sind jedoch neben den in § 110 b OWiG enthaltenen Anforderungen an die elektronische Akte auch die weiteren Regelungen der §§ 110 a ff OWiG über elektronische Dokumente einzuhalten. Wir hätten auch in diesem Fall konkretisierende Regelungen in der Verordnung favorisiert, haben aber dann für die Umsetzung verschiedene Stichpunkte angemerkt und im Übrigen auf die in unserem Gesetzentwurf zum Hamburger Informationsmanagement HIM behandelten Regelungsbedarfe hingewiesen (vgl. II 7).

Die Abstimmung zur Umsetzung dauert an. U.a. haben wir die seit 2009 geführte Diskussion der erforderlichen Speicherdauer zu Rechnungsprüfungszwecken mit der Finanzbehörde wieder aufgegriffen, bei der wir uns seinerzeit an den in Schleswig-Holstein geltenden Regelungen orientiert hatten. Da die Rechnungsprüfung kein eigenes, sondern ein akzessorisches Verfahren ist, muss es grundsätzlich organisatorisch sichergestellt werden, dass in Verfahren, die kurzen gesetzlichen Löschungsfristen unterliegen, auch die Rechnungsprüfung zeitnah erfolgt.

Auftragsdatenverarbeitung im außereuropäischen Ausland:

Ebenfalls im Herbst 2010 hat uns die Anfrage erreicht, ob das erforderliche Einscannen von Postzustellungsurkunden aus fiskalischen Gründen auch durch Unternehmen im außereuropäischen Ausland, hier in Vietnam, vorgenommen werden könne. Dazu hatte die beauftragte deutsche Firma einen Unterauftrag mit einer Ltd. vorgelegt, die sich ihr gegenüber den sog. Standardvertragsklauseln der EU unterworfen hatte. Ausdrücklich hat der betriebliche Datenschutzbeauftragte der Auftragnehmerin eine Beteiligung der hiesigen Aufsichtsbehörde vor diesem Hintergrund für entbehrlich gehalten.

Wir haben dazu auf folgendes hingewiesen und von einer Verarbeitung dort dringend abgeraten:

Nach § 4 des Hamburgischen Datenschutzgesetzes (HmbDSG) sind Auftragnehmer außerhalb der EU datenschutzrechtlich dritte Stellen, so dass die Voraussetzungen für eine Übermittlung ins Ausland gegeben sein müssen, in diesem Fall nach § 16 HmbDSG für eine Übermittlung an private Stellen. Tatsächlich ist aber eine Datenverarbeitung im außereuropäischen Ausland datenschutzrechtlich nicht erforderlich, da die Arbeiten auch durch die Behörde selbst oder im Wege der Auftragsdatenverarbeitung in Deutschland oder wenigstens in Staaten mit ausreichendem Datenschutzniveau erledigt werden können.

Die Unterwerfung unter die EU-Standardvertragsklauseln, die an sich ein gleichwertiges Datenschutzniveau gewährleisten sollen, reicht u. a. deshalb nicht aus, weil darüber nicht wirksam ausgeschlossen werden kann, dass staatliche Zugriffe nach dortigem Landesrecht erfolgen.

Auch wenn unterstellt wird, dass eine preisgünstigere Datenverarbeitung im Ausland grundsätzlich im öffentlichen Interesse liegt, so wäre sie nach § 16 HmbDSG doch nur zulässig, wenn die Betroffenen vorab von der beabsichtigten Datenverarbeitung unterrichtet werden und ihr nicht widersprechen. Der damit verbundene Aufwand dürfte die erwarteten Einsparungen deutlich übertreffen.

Hinzu kommt, dass mit dem sog. Cloud Computing zunehmend nicht mehr hinreichend sicher vorab bestimmt werden kann, wo die Daten tatsächlich verarbeitet werden. Die Einhaltung der datenschutzrechtlichen Anforderungen kann damit nicht gewährleistet werden.

Schließlich entspricht es unserer ständigen Praxis, dass regelmäßig eine Vorabprüfung von Verträgen mit Standardvertragsklauseln durch uns als Aufsichtsbehörde nach § 38 des Bundesdatenschutzgesetzes erforderlich ist.

Nach diesen Hinweisen hat das Projekt mitgeteilt, dass der Auftragnehmer die Verarbeitung nun in Deutschland vornimmt.

14.3 Automationsprojekte im Landesbetrieb Verkehr

Eine frühzeitige und intensive Einbindung von Datenschutzfragen hat sich bewährt.

Seit langem steht der Landesbetrieb Verkehr (LBV) laufend mit verschiedenen Automationsprojekten in Abstimmung mit uns (vgl. 20. TB, 17, 21.TB 17.3, 22. TB, 14.1). Auch im Berichtszeitraum sind wieder unter frühzeitiger Beteiligung mehrere Verfahren behandelt worden, wobei diesmal die Modernisierung der Fachverfahren ComZu (KFZ-Zulassung) und Fahrerlaub-

nis unter dem übergeordneten Projektnamen IT 2010 + x im Vordergrund standen.

1. Das neue IT-Verfahren zur Fahrzeugzulassung

   Mit diesem Projekt ist die Ablösung des alten Zulassungsverfahrens ComZu betrieben worden. Grundlage ist ein Verfahren, das bereits in Hessen eingesetzt worden war und den Hamburgischen Anforderungen angepasst worden ist. Wir haben insbesondere auf den Schutzbedarf für Daten bei Haltern mit eingetragener Meldesperre bzw. Tarnkennzeichen hingewiesen. Dieser wird nun über die Zuordnung von Klarnamen nur außerhalb des elektronischen Systems sowie ein zusätzliches Spezialprofil und ein zusätzliches Kennwort innerhalb des elektronischen Verfahrens abgesichert.

   Ebenfalls haben wir die Frage behandelt, inwieweit nach den neu anzuwendenden Bundesvorschriften im KFZ-Steuerrecht, die die Entrichtung vor Zulassung fordern, zur Verifizierung der Kontodaten bei Lastschrifteinzug eine Schufa-Anfrage durchgeführt werden könne. Hintergrund ist die Minimierung des Ausfallrisikos für die Hamburgische Verwaltung gewesen. Diese Frage haben wir insbesondere deshalb verneint, weil mit der Anbindung an die Bezahlfunktionen im Hamburg-Gateway eine Möglichkeit zur unbaren Zahlung vor Zulassung bereits besteht, aber auch, weil die Schufa sich eine Nutzung der Daten zu eigenen Zwecken vorbehält und nicht sichergestellt werden konnte, dass tatsächlich alle abzufragenden Personen bei der Schufa bereits vorab bekannt sind. Anderenfalls läge in der Anfrage eine unzulässige Übermittlung an private Dritte.

   Leider unterstützt das Verfahren die Trennung von Register und unterstützendem Fachverfahren nicht.

   Im Zuge der Festlegung der technischen und organisatorischen Schutzmaßnahmen ist unter unserer Beteiligung auch ein Verfahren festgelegt worden, wie, ausgehend vom Produktivdatenbestand, ein anonymisierter Testdatenbestand erzeugt wird, der für den Freigabeprozess bei der Migration, aber auch für Softwareanpassungen genutzt werden kann. Auf diese Weise kann zukünftig auf Tests mit Echtdaten verzichtet werden.

2. Das neue IT-Verfahren zur Führerscheinbearbeitung

   Dieses Verfahren löst das bisherige Fahrerlaubnisverfahren ab. Auch hierfür hat man auf das in Hessen eingesetzte Verfahren aufgebaut. Neben den normalen Fahrerlaubnissen werden in diesem Verfahren auch die Fahrlehrererlaubnisse und die Ausgabe der Kontrollgerätekarten (elektronische Tachografen) verwaltet.

Nach unserer Auffassung ergibt sich ein hoher Schutzbedarf bereits aus dem Charakter der Fahrerlaubnisse: Sie gelten lebenslang, und ihr Schicksal ist im Rahmen des gesetzlichen Verbots mit Erlaubnisvorbehalt mit allen Erweiterungen und Entziehungen dauerhaft nachvollziehbar zu speichern. Insoweit sind insbesondere die Integrität und die Revisionsfähigkeit der Daten sicherzustellen. Wir haben hierzu verschiedene technische Anforderungen gestellt. Wir haben angeregt, dass für dieses Verfahren ein Security Service Level Agreement (SSLA) mit dem Dienstleister abgeschlossen wird, damit die Schutzmaßnahmen aller genutzter Komponenten sich einheitlich an dem hohen Schutzbedarf ausrichten. Dazu gehört auch die Nutzung sog. gehärteter Server.

3. Projekt Deutschland online KFZ (Ummeldung)

Im Rahmen des bundesweiten Projekts Deutschland online KFZ Stufe I besteht seit 2011 durch Änderung des Straßenverkehrsgesetzes, der Fahrzeugzulassungsverordnung (FZV) und einer Landesausnahmeverordnung von der FZV im Rahmen einer Experimentierklausel für die Länder die Möglichkeit, durch Online-Angebote die An-, Ab- und Ummeldungen von KFZ für Bürger zu vereinfachen. Eine medienbruchfreie Nutzung kann auch über das Pilotprojekt noch nicht erfolgen. Diese wird weiter im Projekt Deutschland online KFZ Stufe II vorbereitet.

Der LBV hatte unabhängig von diesem bundesweiten Vorhaben in der Vergangenheit bereits zwei online-Angebote entwickelt, die Erleichterungen für Bürger bei der Ummeldung und für sog. Großkunden bei der An- und Abmeldung für sie oder ihre Kunden ermöglichen (vgl. 21.TB, 17.3, 22. TB, 14.1). Vor diesem Hintergrund hat der LBV im Rahmen des Pilotprojekts das Angebot seiner Online-Ummeldungen verbessert. Die Rechtsänderungen ermöglichen es jetzt, dass die Ausstellung der Zulassungsbescheinigungen und damit auch die dafür erforderlichen Prüfschritte wie Abgleich von Meldeanschrift, Versicherungsbescheinigung und KFZ-Daten mit den zuständigen Stellen schon vor der Zulassung verbindlich vorgenommen werden können. Nach wie vor müssen die Betroffenen jedoch vorsprechen, um das Fahrzeug identifizieren zu lassen und die Papiere und Schilder abzuholen. Überlegungen, dies über Lieferdienste oder dritte Stellen wie die Post vornehmen zu lassen, hat der LBV aus Rechtsgründen nicht weiter verfolgt. Wir hatten wiederholt darauf hingewiesen, dass dies nur bei einer Beleihung dieser Stellen möglich wäre, was weitere Rechtsänderungen erfordert hätte.

Sobald die Nutzung des elektronischen Identitätsnachweises, der Bestandteil der neuen Personalausweise ist, über HamburgGateway möglich ist, plant der LBV diese Funktionalität auch für die Online-Angebote des LBV zu nutzen. Diese Planung wird von uns sehr begrüßt, da die

Prozesse dann sowohl datenschutzgerechter als auch benutzerfreundlicher abgewickelt werden können.

15. Wirtschaftsverwaltung

15.1 Modernisierung der Gewerbeüberwachung

Die Einführungsphase des Gewerbeüberwachungsverfahrens mit den Komponenten migewa und eGewerbe ist bis auf Teilbereiche abgeschlossen. Nicht alle Fragen konnten im Rahmen unserer Beteiligung geklärt werden. Daher wird sich eine Prüfung anschließen.

Bei der Modernisierung des Gewerbeüberwachungsverfahrens (vgl. 22. TB, III 15.2) sind wir weiterhin an den vielschichtigen Fragestellungen laufend beteiligt worden. Zwischenzeitlich sind die einzelnen Komponenten weitgehend in Echtbetrieb, und wir haben allen angeschlossenen Stellen für 2012 eine Prüfung des Verfahrens angekündigt.

Im Berichtszeitraum sind insbesondere folgende Fragestellungen vertieft behandelt worden:

1. Entwicklung eines Weiterleitungskonzepts für Daten aus den Gewerbeanzeigen:

   Nach § 14 der Gewerbeordnung (GewO) sind vielfältige und vielgestaltige Formen der Übermittlung von Anzeigendaten zu bewerkstelligen. Mit der Behörde für Wirtschaft, Verkehr und Innovation (BWVI) haben wir ein Konzept entwickelt, das diese Anforderungen datenschutzgerecht abbilden soll.

   Streitig geblieben ist weiterhin, ob öffentlichen Wettbewerbsunternehmen und privaten Stellen ein automatisiertes Abrufverfahren eingerichtet werden darf, obwohl nach § 14 Absatz 8 GewO (zitiert wird jeweils in der nach § 158 GewO noch anzuwendenden Fassung) schon für eine einfache Übermittlung an diese Gruppe die Glaubhaftmachung eines rechtlichen Interesses und nicht nur die Darlegung eines wirtschaftlichen Interesses, wie es in § 29 BDSG Voraussetzung ist.

   Wir hatten bereits im letzten Bericht grundsätzliche Überlegungen dazu behandelt (22. TB, aaO). Das Projekt hat unter Verweis auf eine außerhamburgische Anwendung die Auffassung vertreten, dass der Satz „Ich versichere, dass ich ein rechtliches Interesse habe“ den Anforderungen des § 14 Absatz 8 GewO genüge.

   Für Versicherungen an Eides statt sind jedoch die Anforderungen der §§ 274 Zivilprozessordnung (Angebot aller üblichen Beweismittel oder nachrangig auch eine Versicherung an Eides statt) und § 27 des Hamburgischen Verwaltungsverfahrensgesetzes (Strafbarkeitsbelehrung,

Erklärung zur Niederschrift vor einem Beamten mit der Befähigung zum Richteramt) zu beachten. Diese lassen sich im Rahmen eines Abrufverfahrens nicht abbilden.

Gleiches gilt für Dokumente, die zur Glaubhaftmachung vorgelegt werden.

2. Einsatz einer Sharepoint-Lösung:

§ 14 Absatz 9 GewO gestattet es den Gewerbeüberwachungsbehörden, Daten aus den Gewerbeanzeigen an die dort näher bestimmten Stellen zu übermitteln. Dies ist früher in Papierform erledigt worden und sollte dann per E-Mail erfolgen, darf nach dem Gesetz aber nun auch im Wege eines automatisierten Abrufs erfolgen. Durch die Abschaltung der sogenannten erweiterten Sicherheit im FHH-Netz (siehe II 4) ist die erforderliche Verschlüsselung von E-Mails nicht mehr möglich. Deshalb ist im Frühjahr 2010 die Frage an uns herangetragen worden, ob man als Übergangslösung diese Übermittlungen und die notwendigen verschiedenen sonstigen Übermittlungen nach § 14 GewO an beteiligte Hamburgische Kernbehörden innerhalb des FHH-Netzes vorläufig auch im Wege der Einstellung auf einen Sharepoint bedienen könne, wenn die jeweils zu übermittelnden Daten im Rahmen eines Rollenkonzepts abschließend definiert seien.

Dies haben wir im Sinne einer kurzfristigen Übergangslösung für vertretbar gehalten.

Tatsächlich bildet die Sharepoint-Lösung die rechtlichen Voraussetzungen eines automatisierten Abrufverfahrens aber nicht zutreffend ab, so dass angesichts der Dauer, der Vielzahl und der Unterschiedlichkeit der betroffenen Fälle die Nutzung nun differenziert erfolgen muss:

Während Daten im Abrufverfahren von der Daten haltenden Stelle lediglich in ihrem eigenen Bereich zur „Abholung“ bereitgehalten werden und der Abruf im konkreten Einzelfall vielleicht erst nach Jahren oder auch überhaupt nicht erforderlich wird, müssen die Daten bei der Sharepoint-Lösung laufend händisch zu sog. zip-Dateien gepackt und auf einem Server zur Abholung zur Verfügung gestellt werden. Das Speichervolumen ist nach Auskunft des Projekts bei den anfallenden Datenmengen bereits nach ca. einem Monat erschöpft, so dass viele berechtigte Stellen die Datenpakete „vorsorglich“ abholen, damit sie im Bedarfsfall nicht schon „weg“ sind. Dies ist ein sehr fehleranfälliges Verfahren, und es wäre auf die Dauer eine nicht hinnehmbare unzulässige Datenverarbeitung auf Vorrat. Vertretbar ist das Verfahren nur für solche Fälle, bei denen alle Übermittlungsvoraussetzungen bereits zum Zeitpunkt der Einstellung der Daten auf den Sharepoint vorliegen.

Wir haben deshalb für das Projekt aufgelistet, für welche Kategorien bei einer längerfristigen Nutzung nach § 14 GewO der Sharepoint genutzt und bei welchen Kategorien auf das klassische Abrufverfahren nicht verzichtet werden kann. Wegen der besonderen Gefährdungen ist die Sharepoint-Anwendung im Rahmen der Vorabkontrolle noch gesondert zu betrachten.

3. Online-Anzeige:

   Mit der Online-Gewerbeanzeige wird bisher ein Verfahren angeboten, das wegen des geltenden Schriftformerfordernisses nur vorbereitenden Charakter hat: Die Betroffenen können die Anzeigenformulare downloaden, am PC ausfüllen, ausdrucken und anschließend in Papierform an die zuständige Stelle übersenden. Der Einsatz einer qualifizierten elektronischen Signatur, die eine medienbruchfreie Anzeige ermöglichen würde, wird bisher nicht unterstützt.

   Mit dem Gesetz zur Änderung gewerberechtlicher Vorschriften ist das Schriftformerfordernis entfallen und die Ausgestaltung der Anforderungen landesrechtlichen Verordnungen vorbehalten worden. Eine Regelung steht jedoch noch aus. Damit könnte eine medienbruchfreie Online-Anzeige erleichtert werden. Wir haben das Projekt darauf hingewiesen, dass dann nach § 8 Absatz 2 des Hamburgischen Datenschutzgesetzes erhöhte Anforderungen an das Verfahren, u. a. an die Authentifizierung der Anzeigenden zu stellen sein werden.

4. Kammeranbindung:

   Während des Berichtszeitraums hat es vielfältige Rechtsänderungen gegeben, nach denen letztlich sowohl die Handelskammer Hamburg als auch die Handwerkskammer Hamburg mit der Entgegennahme und Bestätigung von Gewerbeanzeigen betraut worden sind und nach denen sie parallel auch noch als Einheitlicher Ansprechpartner im Sinne der EG-Dienstleistungsrichtlinie u. a. auch andere Anträge nach der Gewerbeordnung entgegennehmen, weiterleiten und Fristen überwachen können.

   Die BWVI hat uns hinsichtlich der Betrauung im Gewerbeanzeigenverfahren nach dem hier einschlägigen Gesetz zur Betrauung sonstiger Stellen mit Aufgaben nach der Gewerbeordnung mitgeteilt, dass den Kammern für diese Aufgabe jeweils Arbeitsplätze analog eines Telearbeitsplatzes zur Verfügung gestellt worden sind.

   Wie andere Behörden auch, haben die Kammern bei der Erfüllung verschiedener Aufgaben nach verschiedenen Gesetzen die jeweils dazu gehörigen Datenbestände strikt zu trennen. Wir haben angekündigt, die konkrete Ausgestaltung des Verfahrens vor Ort zu prüfen.

5. Aufbau eines Testdatenbestandes:

   Wir hatten das Erfordernis eines angemessenen Testdatenbestandes für dieses Verfahren bereits problematisiert (22. TB, 15.2).

   Mit dem Projekt ist die Erforderlichkeit auch für künftige Verfahrensänderungen weiter vertieft worden, und nach verschiedenen Meldungen zum Erfordernis der Testung mit Echtdaten in den einzelnen Teilprojekten ist eine weitere Beratung vereinbart worden.

16. Ausländerwesen

16.1 Elektronische Ausländerakte und Novellierung der Ausländerdatenverarbeitungsverordnung

Die elektronische Ausländerakte bedarf nach ihrer Einführung noch einer hinreichenden Rechtsgrundlage und weiterer technisch-organisatorischer Maßnahmen zur Sicherung der Betroffenenrechte.

Bereits im Jahre 2008 war das Projekt „Elektronische Ausländerakte ELEKTRA“ eingesetzt worden. Ziel war es, die elektronische Akte in das bestehende Fachverfahren PaulaGo(!) zu integrieren und darüber gleichzeitig den Service für alle beteiligten Stellen zu erhöhen. Das Fachverfahren wird als gemeinsame Datei betrieben und wird in der Ausländerdatenverarbeitungsverordnung (AuslDVV) geregelt. Soll das Verfahren durch das Modul einer elektronischen Aktenführung ergänzt werden, ist auch die AuslDVV entsprechend zu ergänzen und das Gesamtverfahren wegen einer wesentlichen Änderung einer erneuten Risikoanalyse zu unterziehen.

Die uns vorgelegten Überlegungen befassten sich zunächst mit der Nutzung durch die an das Verfahren angeschlossenen Ausländerdienststellen. Neben der einfachen Digitalisierung der vorhandenen Akten durch Scannen wurden für einzelne Dokumente elektronische Signaturen eingeplant. Dies betraf vor allem Dokumente mit gesetzlich vorgeschriebener Schriftform und die ausländerrechtlichen Titel. Dazu wurden einzelne technische Aspekte mit dem Projekt erörtert.

Im Frühjahr 2010 wurde an uns die Frage herangetragen, in welcher Form eine Einbindung dritter Dienststellen, die aus unterschiedlichen Gründen bisher die kompletten Akten zur Einsicht erhalten hätten, erfolgen könne. Hierzu gaben wir allgemeine Hinweise.

Zunächst haben wir uns bei der Betrachtung in den Grundzügen an den Überlegungen, die bis dahin auch das behördenübergreifende Projekt zur Einführung elektronischer Akten ELDORADO bestimmten, orientiert. Erst mit fortschreitender Diskussion zur Digitalisierung von Akten und deren

Einbindung in den Workflow (siehe II 6, III 14.1) zeichneten sich aus den spezifischen Risiken als führendes und letztlich alleiniges Speichermedium eine Reihe weiterer rechtlicher Anforderungen ab.

In dieser Phase erreichte uns ein erster Entwurf zur Änderung der AuslDVV, gegen den wir aus mehreren Gründen Bedenken hatten. Besonders schwerwiegend war, dass ausgehend von der unzutreffenden Überlegung, die elektronische Ausländerakte sei als Teil des Verfahrens PaulaGo(!) keine automatisierte Datei, der erste Entwurf vorsah, neben 21 verschiedenen Dienststellen von Behörde für Inneres und Sport, Justizbehörde, Staatsanwaltschaften und Gerichten auch dem Verfassungsschutz jeweils die gesamte Ausländerakte ungeprüft im Wege des automatisierten Abrufs zur Verfügung zu stellen. Es wurde deutlich, dass die Abwägung mit den schutzwürdigen Betroffeneninteressen entgegen der gesetzlichen Verpflichtung in § 14 Absatz 2 des Hamburgischen Datenschutzgesetzes nicht vorgesehen war. Dieser Entwurf wurde auch wegen der Kritik anderer Behörden nicht weiter verfolgt.

In einem zweiten Entwurf waren Abrufe nicht mehr vorgesehen. Es waren aber immer noch die prägenden Grundsätze des Datenschutzrechts wie die Erforderlichkeit einzelner Datenübermittlungen nicht gewährleistet. Mit der Digitalisierung und automatisierten Verarbeitung der Akten steigen die datenschutzrechtlichen Risiken für die Betroffenen durch schnelleren Zugang, leichtere Vervielfältigungsmöglichkeiten usw. Die Daten verarbeitende Stelle muss sicherstellen, dass auch unter diesen Umständen die Datenschutzvorschriften eingehalten werden. Geschützt ist jedes einzelne Datum der Betroffenen. Unzulängliche Technik und mangelnde Personalkapazitäten können nicht dazu führen, materiell unzulässige Datenverarbeitung zu legitimieren. Automatisierte Verfahren dürfen daher nur betrieben werden, wenn sie diese rechtlichen Anforderungen exakt abbilden. Dies gilt zumindest für so sensible Bereiche wie die Ausländerakte, die lebenslang geführt wird.

Schließlich sind auch Fragen der technisch-organisatorischen Absicherung angesichts des unbestreitbar hohen Schutzbedarfs, wie etwa die dauerhafte Dokumentation einzelner Zugriffe am Datensatz, strikte Zweckbindung und Beweisbarkeitsanforderungen ebenso offen geblieben wie Stichprobenkontrollen und die Dokumentation von Zuständigkeitswechseln.

Auch zu diesem Entwurf haben wir der Behörde verschiedene Änderungsvorschläge unterbreitet.

Kurz vor Redaktionsschluss ist uns ein weiterer Entwurf zugegangen. Auch dieser sieht jedenfalls für Teilbereiche im Ergebnis immer noch die elektro-

nische Übersendung der ganzen Akte vor. Wir werden diesen Entwurf kritisch prüfen und uns weiterhin für eine an der Erforderlichkeit ausgerichtete, verhältnismäßige Verarbeitung und weitere Datenschutzverbesserungen einsetzen.

17. Melde- und Personenstandswesen

17.1 Neuer Entwurf eines Bundesmeldegesetzes

Mit dem neuen Entwurf eines Bundesmeldegesetzes wurde erneut die Chance, ein modernes, den datenschutzrechtlichen Prinzipien verpflichtetes Melderecht zu schaffen, welches dem Bürger mehr Rechte als bisher einräumt, vertan.

Im Zuge der Föderalismusreform im Jahre 2006 wurde das Meldewesen in die ausschließliche Gesetzgebungskompetenz des Bundes überführt.

Wie schon beim Referentenentwurf für ein Bundesmeldegesetz aus dem Jahr 2008 (BMG-E 2008) (vgl. dazu 22. TB, 17.) wurde auch durch den aktuellen Entwurf die Gelegenheit, das Melderecht datenschutzfreundlicher zu gestalten, nicht ergriffen. Insbesondere wird das Recht auf informationelle Selbstbestimmung des Bürgers bei einfachen Melderegisterauskünften und Melderegisterauskünften in besonderen Fällen nicht hinreichend geschützt. Durch den Bundesdatenschutzbeauftragten erfolgte gegenüber dem Bundesinnenministerium (BMI) eine mit den Datenschutzbeauftragten der Länder abgestimmte Stellungnahme, die darlegt, dass auch im neuen Referentenentwurf die Belange des Datenschutzes sowohl aus rechtlicher als auch technischer Sicht nicht hinreichend berücksichtigt werden. Die von den Datenschutzbeauftragten erhobene Kritik und die aufgestellten Forderungen wurden leider in dem nunmehr bereits vorliegenden Gesetzentwurf der Bundesregierung (Drucksache 524/11) nur teilweise aufgenommen und umgesetzt.

Einige Schwerpunkte des Gesetzesentwurfs:

- Zu begrüßen ist, dass mit dem neuen Gesetzentwurf, wie von den Datenschutzbeauftragten seit langem gefordert, auf die Einrichtung eines zentralen Bundesmelderegisters verzichtet wird.
- Durch den neuen Gesetzentwurf ist der Ausbau des Online-Zugangs für öffentliche Stellen, insbesondere durch Abrufverfahren auf bestehende Meldedatenbestände vorgesehen. Als aus datenschutzrechtlicher Sicht nicht ausreichend haben wir hier die getroffenen Regelungen hinsichtlich der Authentifizierung des Empfängers, der Vertraulichkeit, Integrität

und Authentizität der Daten bei der Übermittlung von Meldedaten sowie der Auswahldaten zur sicheren Verifizierung der gesuchten Person kritisiert.

- Des Weiteren wurde der von den Datenschutzbeauftragten erhobenen Forderung, auf die Bildung von Ordnungsmerkmalen entweder gänzlich zu verzichten oder aber diese ausschließlich abstrakt zu bilden und deren Übermittlung zu untersagen, nicht nachgekommen. Dies ist im Hinblick auf die verfassungsrechtlich gebotene Vermeidung eines Personenkennzeichens äußerst kritisch zu sehen.
- Der von den Datenschutzbeauftragten bereits zum BMG-E 2008 erhobenen Forderung, bei einer Neuordnung des Meldewesens den Umfang der im Melderegister gespeicherten Daten einer kritischen Prüfung zu unterziehen und auf die für die meldebehördlichen Kernaufgaben erforderlichen Daten zu beschränken, kommt auch der nun vorliegende Gesetzentwurf nicht nach. Im Gegenteil, der Datenumfang soll sogar zusätzlich erweitert werden. Besonders kritisch sehen wir hier die vorgesehene Speicherung der Steuer-ID und die Speicherung des Sperrkennworts und der Sperrsumme des Personalausweises.
- Auch der Forderung der Datenschutzbeauftragten, einen umfassenden Auskunftsanspruch des Betroffenen hinsichtlich der gespeicherten Daten und der erfolgten Datenübermittlungen zu schaffen, wurde nur zum Teil nachgekommen, indem der Auskunftsanspruch um Datenübermittlungen im Einzelfall im automatisierten Abrufverfahren erweitert wurde. Das Auskunftsrecht des Betroffenen als zentraler Bestandteil des Rechts auf informationelle Selbstbestimmung ist jedoch weder in § 19 BDSG oder den entsprechenden Vorschriften der Landesdatenschutzgesetze auf bestimmte Arten und Formen von Datenübermittlungen beschränkt und sollte im Melderecht keine diesbezügliche Beschränkung erfahren. Nicht ausreichend sind auch hier die Regelungen bezüglich der sicheren Identifizierung des Antragstellers.
- Ebenfalls unbeachtet blieben die seit langem geforderte Abschaffung der sogenannten Hotelmeldepflicht und die damit verbundene millionenfache Datenerhebung auf Vorrat.
- Kritisch bewertet haben wir auch die geplante Wiedereinführung der Mitwirkungspflicht des Wohnungsgebers und die damit verbundene zusätzliche Erhebung und Speicherung von Daten sowohl des Meldepflichtigen als auch des Wohnungsgebers.
- Bei den Regelungen zu Melderegisterauskünften gibt es zwar Verbesserungen, doch ist aus datenschutzrechtlicher Sicht das Recht der

Betroffenen auf informationelle Selbstbestimmung nach wie vor nicht hinreichend geschützt.

Bei der einfachen Melderegisterauskunft macht der Gesetzentwurf die Erteilung einer Melderegisterauskunft zum Zwecke der Werbung oder des Adresshandels nunmehr von der Einwilligung des Betroffenen abhängig und normiert für die Auskunft zu gewerblichen Zwecken eine Zweckbindung. Dies stellt zwar eine Verbesserung dar, setzt letztlich jedoch nur die Vorgaben des Bundesverwaltungsgerichts im Urteil vom 21.06.2006 (Az. 6 C 5/05) um. Unklar bleibt jedoch, ob und wie die Berechtigung zum Erhalt der Auskunft und die Zweckbindung überprüft werden können. Dafür müsste nachvollziehbar sein, wer der Anfragende ist und welche Daten er wann erhalten hat. Erforderlich dafür wären Regelungen über die sichere Authentisierung und Protokollierung der Anfrage, welche bisher fehlen. Auch eine Datenverarbeitung im Auftrag wäre dabei zu berücksichtigen.

Bei den Melderegisterauskünften in besonderen Fällen ist weiterhin nur eine Widerspruchsmöglichkeit statt der geforderten Einwilligung der Betroffenen vorgesehen. Dies führt für Hamburger Bürger zu einer erheblichen Einschränkung ihres informationellen Selbstbestimmungsrechts, da die bisher im HmbMG bestehende Einwilligungslösung in den Fällen der Auskunftserteilung bei Wahlen zur Bürgerschaft und den Bezirksversammlungen und bei Alters- und Ehejubiläen entfallen würde. Eine weitere Verschlechterung stellt die im HmbMG bisher nicht bestehende Möglichkeit der Auskunftserteilung an Adressbuchverlage dar, für die ebenfalls nur eine Widerspruchsmöglichkeit vorgesehen ist.

Es bleibt abzuwarten, ob die von den Datenschutzbeauftragten weiterhin erhobenen Forderungen nach einer datenschutzgerechten Ausgestaltung des Melderechts im weiteren Gesetzgebungsverfahren noch Berücksichtigung finden werden.

17.2 Einführung des Elektronischen Personenstandsregisters

Technische Lösungen zur Umsetzung einer elektronischen Registerführung müssen sich an den rechtlichen Vorgaben orientieren. Zentrale elektronische (Landes-)Registerverfahren dürfen nur auf der Grundlage entsprechender Rechtsgrundlagen eingerichtet werden. Besteht eine solche nicht, sind die Standesamtsdaten strikt getrennt zu halten und zu verarbeiten.

Am 01. Januar 2009 sind das modernisierte Personenstandsgesetz (PStG) und die Verordnung zur Ausführung des Personenstandsgesetzes (PStV) in Kraft getreten. Ein wesentlicher Bestandteil der Gesetzesreform ist die Einführung von elektronischen Personenstandsregistern. Diese werden ab 2014 die bisherigen Personenstandsregister in Papierform ersetzen.

Erlaubt ist die elektronische Registerführung durch den Gesetzgeber bereits seit Januar 2009, verbindlich wird sie für die Standesämter jedoch erst ab 2014.

Innerhalb von 5 Jahren müssen also geeignete technische Lösungen für die Umsetzung entwickelt werden.

Auch nach dem neuen Personenstandsgesetz bleiben die örtlichen Standesämter für die Führung der Personenstandsregister zuständig. Gem. §§ 67 und 74 Abs. 1 Nr. 3 PStG werden die Landesregierungen der Länder jedoch ermächtigt, per Rechtsverordnung auf Länderebene zentrale Personenstandsregister einzurichten und nähere Bestimmungen zu deren Führung zu treffen. Nach den Vorgaben der §§ 67 und 74 Abs. 1 Nr. 3 PStG dürfen die angeschlossenen Standesämter des Bundeslandes die bei ihnen gespeicherten Standesamtsdaten an ein solches zentrales Register übermitteln und diese in dem zentralen Register speichern. Die Führung des Registers obliegt hierbei weiterhin ausschließlich dem zuständigen Standesamt. Den angeschlossenen Standesämtern darf jedoch Einblick in sämtliche Register gewährt werden, um die Ausstellung von Personenstandsurkunden auch durch das örtlich nicht zuständige Standesamt zu ermöglichen. Für die Einrichtung eines länderübergreifenden zentralen Registers besteht auch nach dem neuen Personenstandsgesetz keine rechtliche Grundlage.

Bei dem Personenstandsregister handelt es sich nicht nur um ein Verfahren mit großem Betroffenenkreis und hohem Schutzbedarf, sondern in den Registern werden auch sämtliche anzeigepflichtigen familienrechtlichen Umstände (Geburten, Eheschließungen, Begründungen von Lebenspartnerschaften, Namensführung, Adoptionen) verarbeitet. Bei der Umstellung des Verfahrens und der Archivierung muss der Urkundencharakter der Dokumente erhalten bleiben. Hierbei sind Aufbewahrungszeiten von bis zu 110 Jahren zu realisieren.

Die Länder Hamburg, Schleswig-Holstein und Bremen haben Dataport mit der Entwicklung einer gemeinsamen Lösung und dem Betrieb des Verfahrens länderübergreifend beauftragt. Erklärtes Ziel dieser Kooperation war es, Synergien aus gemeinsamer Entwicklung, Einführung und Betrieb der Lösung zu realisieren.

Nach der vorgelegten Konzeption ist für die drei beteiligten Bundesländer die Nutzung einer Infrastruktur in einem gemeinsamen Verfahren und Rechenzentrumsbetrieb vorgesehen, d.h. es soll künftig ein zentral betriebenes Personenstandsregisterverfahren für alle drei beteiligten Länder in Altenholz und ein Sicherungsregister in Hamburg geben. Die personenstandsrechtlich zwingende Trennung der Standesamtsdaten (§ 3 Abs. 1

PStG) soll über mandantenorientierte, technische und organisatorische Regelungen sichergestellt werden.

Insbesondere vor dem Hintergrund, dass für die Einrichtung eines länderübergreifenden zentralen Registers keine rechtliche Grundlage besteht und in Hamburg bisher keine Entscheidung für die Einführung eines zentralen Landesregisters getroffen und daher keine entsprechende Verordnung erlassen wurde, haben wir nach ersten Gesprächen im November 2010 wiederholt um Darstellung des Konzeptes und der Realisierung der Trennung der Datenverarbeitung auf Landes- und Standesamtsebene gebeten.

Erst im Rahmen der – von uns in Teilen begleiteten – Vorabkontrolle des Unabhängigen Datenschutzzentrums Schleswig-Holsteins wurde uns im September 2011 ein Konzept zur Mandantentrennung und Protokollierung für das elektronische Personenstandsregister übersandt. Die Standesamtsdaten der Standesämter der drei Länder werden demnach physikalisch gemeinsam gespeichert. Die Trennung der Daten erfolgt logisch durch ein länderübergreifendes Berechtigungskonzept.

Die Datenschutzbeauftragten der Länder Bremen, Hamburg und Schleswig-Holstein haben sich intensiv mit dem geplanten Verfahren „Elektronisches Personenstandregister“ auf der Grundlage der bestehenden Rechtsgrundlagen und der vorliegenden Dokumente auseinandergesetzt. Gemeinsam vertreten wir die Auffassung, dass ein IT-Verfahren, in dem die Daten der drei beteiligten Bundesländer gespeichert und verarbeitet werden, nur datenschutzgerecht und gesetzeskonform erfolgen kann, wenn eine Mandantenfähigkeit auf der Grundlage einer getrennten Datenhaltung und -verarbeitung realisiert ist.

Als maßgebliche Kriterien für eine Mandantenfähigkeit werden angesehen:

- Die konfigurative Unabhängigkeit der Mandanten

  Dazu gehört:

  – getrennte Datenhaltung,

  – Einstellungen wie Umfang der zu speichernden Daten, Funktionen und Berechtigungen, Art und Umfang sowie Löschung der Protokolldaten erfolgen mandantenorientiert und dürfen sich nicht auf andere Mandanten auswirken.

- Die Abgeschlossenheit von Transaktionen

  Dazu gehört:

  – Transaktionen dürfen keine Seiteneffekte auf andere Mandanten haben, d.h. Fehler in einem Mandanten dürfen auf andere Mandanten nicht durchschlagen,

  – eine vollständige Löschung oder Deaktivierung eines Mandanten darf nicht dazu führen, dass die Daten anderer Mandanten nicht mehr verarbeitet werden können.

- Das Management für mandantenübergreifende Funktionen und Einrichtungen

  Dazu gehört:

  – Definition eines differenzierten Administrationskonzepts,

  – revisionssichere Protokollierung der administrativen Tätigkeiten und Festlegung eines Protokollierungskonzepts,

  – Definition eines mandantenspezifischen und mandantenübergreifenden Berichtswesens,

  – Definition von Revisionen über das Gesamtsystem,

  – Definition von Prozessen für das mandantenspezifische und mandantenübergreifende Changemanagement.

Die vorliegenden Unterlagen belegen aus unserer Sicht, dass die dargelegten Kriterien einer Mandantenfähigkeit derzeit nicht erreicht werden. Aus diesem Grund haben wir die Auftraggeber und das Projekt in einer gemeinsamen Stellungnahme mit den Datenschutzbeauftragten der Länder Bremen und Schleswig-Holstein aufgefordert, darzulegen, durch welche zusätzlichen technischen Maßnahmen eine getrennte Datenhaltung (z. B. dedizierte Datenbanktabellen in abgeschlossenen Bereichen etc.) und -verarbeitung für die drei beteiligten Länder und die weiteren Kriterien der Mandantentrennung umgesetzt werden sollen.

Bis zum Redaktionsschluss haben wir hierzu keine neuen Unterlagen erhalten.

Wir werden das Verfahren weiter kritisch begleiten.

17.3 Datenpanne bei der Standesamtlichen Registerstelle mit dem Generalregister der Hamburgischen Standesämter

Das Fehlverhalten einer Mitarbeiterin der Standesamtlichen Registerstelle erschüttert das Vertrauen der Bürger in den behördlichen Umgang mit ihren personenbezogenen Daten. Die datenschutzrechtliche Verantwortung muss jedem Mitarbeiter immer wieder bewusst gemacht werden.

In der Standesamtlichen Registerstelle werden Zweitausfertigungen sämtlicher Personenstandsregister der Hamburger Standesämter, die sogenannten Sicherungsregister, verwahrt. Wird in einem Standesamt eine Änderung beurkundet, schickt das Standesamt eine entsprechende Mitteilung an die Standesamtliche Registerstelle, damit dort die Sicherungsregister fortgeführt werden können. Weiterhin wird mit dem Generalregister ein zentrales Suchregister für die Hamburger Standesämter geführt.

Am 15. Juni 2011 wurden wir durch die behördliche Datenschutzbeauftrage für die Bezirksämter und die Presse darüber informiert, dass eine Mitarbeiterin der Standesamtlichen Registerstelle mindestens 375 Mitteilungen verschiedener Standesämter unbearbeitet in einem Müllcontainer entsorgt hatte. Dort wurden die Unterlagen von einem Bürger gefunden und einer Hamburger Tageszeitung zugespielt.

Die Mitarbeiterin wurde durch die Dienststellenleitung umgehend suspendiert, und die Standesamtliche Registerstelle wurde vorübergehend geschlossen. Die im Müll aufgefundenen Dokumente wurden von dem Journalisten an die Registerstelle zurückgegeben.

Wir haben am 16. Juni unter Einbeziehung der behördlichen Datenschutzbeauftragten aus Anlass der unzulässigen Entsorgung von standesamtlichen Unterlagen eine Ad-hoc-Prüfung bei der Standesamtlichen Registerstelle mit dem Generalregister der Hamburgischen Standesämter durchgeführt. Gegenstand der Prüfung waren Aufgaben und Arbeitsabläufe, einschließlich eingerichteter elektronischer Verfahren und die Feststellung des Umfangs und Ausmaßes des durch die unzulässige Entsorgung eingetretenen Schadens. Die Prüfung ist noch nicht abgeschlossen. Die Ergebnisse der Prüfung werden wir im nächsten Tätigkeitsbericht darstellen.

18. Personalausweis- und Passwesen

18.1 Einführung des elektronischen Personalausweises: neue Möglichkeiten, aber auch zusätzliche Risiken

Der neue Personalausweis kann als elektronischer Identitätsnachweis (eID) im Internet genutzt werden. Vom Ausweisinhaber erfordern diese zusätzlichen Möglichkeiten, ein sehr verantwortliches Umgehen mit dem Ausweis nicht nur bei der Nutzung im Internet. Darum sollte der neue Ausweis nicht als Pfand hinterlegt werden.

Seit dem 01. November 2010 wird der neue Personalausweis im Scheckkartenformat ausgegeben. Bei den neuen Personalausweisen sind die auf dem Ausweis sichtbar aufgeführten Daten mit Ausnahme der Unterschrift,

aber einschließlich des biometrischen Gesichtsbildes in einem Chip gespeichert und elektronisch auslesbar.

Über die herkömmliche Ausweisfunktion hinaus, kann der neue Personalausweis auch als elektronischer Identitätsnachweis (eID) im Internet genutzt werden. Die eID-Funktion ermöglicht es dem Ausweisinhaber, sich sowohl im E-Government als auch im E-Commerce gegenüber berechtigten Stellen zu identifizieren. Die Daten, die im Chip auf dem Ausweis gespeichert sind, können nach Zustimmung des Ausweisinhabers mit seiner PIN an einen Internet-Dienst übertragen werden. Diese Funktion soll im Zeitalter des Internets das Alltagsleben erleichtern und den Geschäftsverkehr sicherer machen. Dabei werden stets nur die Daten übertragen, die der Anbieter für die Erbringung seines Dienstes benötigt. Die Datenschutzbeauftragten des Bundes und der Länder haben sich dafür eingesetzt, dass die Dienstebetreiber die datenschutzgerechte Nutzung der übertragenen Ausweisdaten im Vorfeld der Einführung gegenüber dem Bundesverwaltungsamt belegen müssen. Auch die hamburgische Verwaltung plant die Nutzung der eID, um ihre E-Government-Angebote sicherer und benutzerfreundlicher zu gestalten. Eine erste Nutzungsmöglichkeit soll jedoch erst im zweiten Quartal 2012 zur Verfügung stehen.

Um die eID-Funktion am PC nutzen zu können, benötigt man einen Kartenleser. Bürgerinnen und Bürger, die diese Funktion nutzen wollen, sollten sich einen Komfortleser anschaffen, der über eine eigene Tastatur zur Eingabe der PIN und ein Display verfügt. Nur wenn man einen Komfortleser nutzt, kann verhindert werden, dass Hacker die PIN-Eingabe abfangen und missbrauchen können. Die einfachen Basis-Lesegeräte, die von der Bundesregierung in großer Stückzahl kostenlos zur Verfügung gestellt wurden, erfüllen diese Datenschutzanforderung nicht. Von ihrem Gebrauch ist abzuraten.

Neben dem Lichtbild können auch Fingerabdrücke auf dem neuen Personalausweis gespeichert werden. Dies ist jedoch eine freiwillige Option und darf nur mit schriftlicher Einwilligung der Betroffenen erfolgen. Darauf sind die Antragsteller durch die Ausweisbehörde schriftlich hinzuweisen. Mit der Preisgabe und Speicherung der Fingerabdrücke als äußerst sensible Daten werden Missbrauchsrisiken eröffnet, denen kein gravierender Vorteil des Ausweisnutzers gegenübersteht. Daher sollte sich jeder Antragsteller genau überlegen, ob er seine Fingerabdruckdaten auf dem Personalausweis speichern lassen will.

Eine weitere neue Funktion ist die Unterschriftsfunktion. Mit der elektronischen Signaturfunktion können u. a. Verträge, die eine eigenhändige Unterschrift erfordern, über das Internet geschlossen werden. Während

man bisher eine spezielle Signaturkarte brauchte, soll die Signatur nun auf dem Chip des Personalausweises gespeichert werden können. Diese Option wurde jedoch zurückgestellt und soll voraussichtlich erst 2012 ergänzt werden. Eine Speicherung dieser Signatur auf dem Chip des Personalausweises erfolgt dann jedoch nur, wenn der Ausweisinhaber dies möchte und er sich die Signatur nach der Ausgabe des Ausweises zusätzlich besorgt.

Die neuen elektronischen Funktionen des Personalausweises bieten zwar neue Möglichkeiten. Es bedarf aber auch mehr Verantwortung im Umgang mit dem neuen Ausweis. Dies hat auch der Gesetzgeber erkannt. Nach dem neuen Personalausweisgesetz darf vom Ausweisinhaber grundsätzlich nicht mehr verlangt werden, den Ausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben. Eine sonst in manchen Bereichen übliche Hinterlegung des Personalausweises als Pfand ist damit jetzt unzulässig.

18.2 Antragsverfahren für ePass und neuen Personalausweis weist immer noch gravierende Mängel auf

Die Mängel im Antragsverfahren für den elektronischen Reisepass, die im Zuge der Einführung des neuen Personalausweises beseitigt werden sollten, sind nach wie vor vorhanden.

Anlässlich der Prüfung des Antragsverfahrens für den elektronischen Reisepass (ePass) hatten wir bereits 2008 festgestellt, dass dieses Verfahren zwei gravierende Mängel aufweist (vgl. 22. TB, 18.1):

- Die zu einem Pass erhobenen Passantragsdaten könnten nach der Erfassung verändert werden. Die Fingerabdruckdaten könnten z. B. ausgetauscht werden, ohne dass dies auffallen würde.

  Wir haben bereits 2008 die Forderung erhoben, dass unmittelbar nach der Erfassung der jeweiligen Antragsdaten sowohl eine gewollte als auch ungewollte Veränderung sowie ein Austausch einzelner Daten durch technische Maßnahmen ausgeschlossen werden sollten.

  In der Mitteilung des Senats an die Bürgerschaft „Stellungnahme des Senats zum 22. Tätigkeitsbericht des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit“ 19/7193 vom 07.09.2010 wird dazu ausgeführt: „Die vom HmbBfDI geforderte technische Verknüpfung aller Passantragsdaten eines Antragstellers wird mit der Überarbeitung des technischen Fachverfahrens im Rahmen der Einführung des neuen Personalausweises zum 1. November 2010 realisiert“. Die Fachliche Leitstelle hat im Oktober 2010 diese Zusage konkretisiert und deren technische Umsetzung dargelegt.

- Des Weiteren war bereits 2008 von uns festgestellt worden, dass die gesetzlich vorgegebenen Löschungsfristen für die Fingerabdruckdaten beim ePass nicht eingehalten werden.

  Auch dieser Mangel sollte im Zuge der Einführung des neuen Personalausweises beseitigt werden.

Bei einer Prüfung des Antragsverfahrens zum neuen Personalausweis und ePass haben wir im Juni 2011 jedoch festgestellt, dass die in der Stellungnahme des Senats zum 22. Tätigkeitsbericht zugesagte Mängelbeseitigung nicht erfolgt ist. Obwohl die Fachliche Leitstelle aus den zahlreichen Kontakten mit uns um die Bedeutung gerade dieser geforderten Maßnahmen wusste, hat sie es versäumt, diese Punkte mit uns im Vorfeld der Einführung der neuen Version des IT-Verfahrens offen zu kommunizieren. Nach eigenen Aussagen wusste die Fachliche Leitstelle nicht, dass der Softwarehersteller die angekündigte Veränderung nicht realisiert hat. Ein solches Vorgehen der Fachlichen Leitstelle ist äußerst kritisch zu bewerten. Die Fachliche Leitstelle hat dieses eingeräumt und zugesagt, dass zukünftig die zugesagten Maßnahmen im Zuge der Freigabe des IT-Verfahrens explizit getestet werden sollen. Die von uns geforderte Bindung der Antragsdaten soll nunmehr spätestens im November 2012 realisiert werden. Auch hinsichtlich der Löschung der Fingerabdruckdaten soll das derzeitige Verfahren verändert werden, so dass dann die gesetzlichen Vorgaben eingehalten werden. Wir werden diese Verfahren weiter kritisch begleiten.

19. Statistik

19.1 Registergestützte Volkszählung – Zensus 2011

Auch nach Abschluss der Befragungen muss die datenschutzgerechte Durchführung des Zensus 2011 sichergestellt werden. Insbesondere werden wir die Einhaltung der gesetzlichen Löschfristen für die identifizierenden Hilfsmerkmale überwachen.

Der Deutsche Bundestag hat im Jahr 2009 aufgrund der EU-Verordnung vom 09. Juli 2008 (Verordnung EG Nr. 763/2008) mit dem Zensusgesetz 2011 eine Volkszählung beschlossen. Bereits im Vorfeld der Volkzählung erfolgten auf der Grundlage des im Dezember 2007 verabschiedeten Zensusvorbereitungsgesetzes (ZensVorG 2011) umfangreiche Vorbereitungen und Datensammlungen (vgl. dazu 21. TB, 5.2). Durch das ZensVorG 2011 wurde insbesondere der Aufbau eines Anschriften- und Gebäuderegisters geregelt und festgelegt, welche Daten die Behörden aus ihren Registern dem Statistischen Bundesamt und den Statistischen Landesämtern zu übermitteln haben.

Der Zensus 2011 unterscheidet sich in der Methode wesentlich von vorangegangenen Volkszählungen, wie sie zuletzt 1987 auf dem früheren Bundesgebiet und 1981 in der ehemaligen DDR stattgefunden haben. Anders als bei diesen traditionellen Volkzählungen, bei denen sämtliche Bürger befragt wurden, werden beim Zensus 2011 vor allem vorhandene Verwaltungsregister, wie die Melderegister, Register der Bundesagentur für Arbeit und erwerbsstatistische Daten öffentlicher Arbeitgeber genutzt und ausgewertet und nur ergänzend ein Teil der Bevölkerung befragt. Man spricht von einem sogenannten „registergestützten Zensus".

Mit dem Zensus 2011 sollen nicht nur Daten zur Bevölkerung und deren Erwerbssituation, sondern auch zur Wohnsituation der Menschen erhoben werden. Daher wird auch eine Gebäude- und Wohnungszählung durchgeführt, bei der etwa 17,5 Millionen Eigentümerinnen und Eigentümer von Wohnraum postalisch befragt werden. Im Rahmen der ergänzenden Haushaltebefragung werden etwa 7,9 Millionen (in Hamburg ca. 62.500) Menschen befragt. Da sich die beiden Gruppen überschneiden, wird etwa ein Drittel der Bevölkerung Auskunft geben müssen. Außerdem erfolgt direkt vor Ort die Erhebung von Daten über die Bewohner von Gemeinschaftsunterkünften und die Insassen der Justizvollzugsanstalten.

Stichtag für den Zensus 2011 war der 09. Mai 2011. An diesem Tag haben die Befragungen begonnen. Man rechnet damit, dass die Befragungen einschließlich aller Rückfragen bis zum April 2012 abgeschlossen sein werden. Der Beginn der Befragungen führte dazu, dass sich viele Bürger mit Eingaben und Anfragen an uns gewandt haben. Um auch dem großen Informationsbedürfnis der Bürger nachkommen zu können, haben wir Informationen zum Zensus 2011 und Antworten auf die meist gestellten Fragen (FAQ) auf unserer Homepage veröffentlicht.

Die Volkszählung Zensus 2011 wurde von den Datenschutzbeauftragten des Bundes und der Länder von Anfang an intensiv und kritisch begleitet. Datenschutzrechtliche Aspekte wurden in einer für den Zensus 2011 einberufenen Arbeitsgruppe unter den Datenschutzbeauftragten des Bundes und der Länder diskutiert und datenschutzrechtliche Forderungen gegenüber der amtlichen Statistik erhoben. Wir haben mit dem Statischen Amt für Hamburg und Schleswig-Holstein in einer Vielzahl von Gesprächen datenschutzrechtliche und technische Fragestellungen bei der Durchführung des Zensus 2011 erörtert.

Der bereits im Rahmen des Gesetzgebungsverfahrens zum Zensusgesetz 2011 von den Datenschutzbeauftragten aufgestellten Forderung, auf das Erhebungsmerkmal „Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgemeinschaft" zu verzichten, kam der Gesetzgeber nicht nach. Der

Datenkatalog wurde sogar noch um die Frage nach dem „Bekenntnis zu einer Religion, Glaubensrichtung oder Weltanschauung“ erweitert, wobei die Beantwortung dieser weiteren Frage freigestellt wurde. Bei den Angaben zu einer Religions- oder Glaubenszugehörigkeit oder einer Weltanschauung handelt es sich um sehr sensible Daten, welche auch durch die Datenschutzgesetze des Bundes und der Länder besonderen Schutz erfahren. Gleichwohl ist der Gesetzgeber dem Wunsch der öffentlich-rechtlichen Religionsgesellschaften nach Aufnahme dieser Fragen in den Fragenkatalog des Zensus 2011 nachgekommen, obwohl die Erhebung dieser besonders sensiblen Daten durch die EG-Verordnung nicht vorgeschrieben ist.

Auch die Forderung aus Datenschutzkreisen, in sensiblen Sonderbereichen wie etwa Justizvollzuganstalten auf eine Erhebung zu verzichten, fand kein Gehör. Allerdings wurde durch die amtliche Statistik hierfür ein spezielles Verfahren entwickelt. Dieses sieht vor, dass an den sensiblen Sonderbereichen nur Erhebungen zur Feststellung der amtlichen Einwohnerzahl stattfinden. Dazu sind die Anstaltsleitungen darüber zur Auskunft verpflichtet, welche Personen sich in der Anstalt befinden. Weiterhin war eine frühzeitige sukzessive Löschung der identifizierenden Hilfsmerkmale vorgesehen. Der zuvor erforderliche Meldedatenabgleich für die sensiblen Sonderbereiche sollte deshalb wesentlich früher stattfinden als der Abgleich für sonstige Anschriften, damit eine schnellstmögliche Anonymisierung erreicht werden kann. Umso bedauerlicher ist daher, dass aufgrund verspätet fertiggestellter Softwareprogramme dieses Verfahren derzeit nicht wie vorgesehen durchgeführt werden kann und der geplante Löschtermin für die identifizierenden Hilfsmerkmale zum 31. Dezember 2011 nicht eingehalten werden wird.

Weitere bei der Durchführung des Zensus 2011 aufgetretene datenschutzrechtliche Probleme und Fragestellungen sind:

- Das Wiederaufleben des Auskunftsanspruches der Betroffenen über die zu ihrer Person gespeicherten Daten nach den Datenschutzgesetzen des Bundes und der Länder aufgrund der besonderen Datenerhebung beim Zensus 2011, wonach Daten nicht ausschließlich bei den Betroffenen, sondern auch aus Verwaltungsregistern erhoben wurden. Für die Datenverarbeitung durch das Statistische Amt für Hamburg und Schleswig-Holstein führte dies nicht zu einer Auskunftspflicht, da nach § 18 Abs. 3 HmbDSG ein Auskunftsanspruch nicht besteht, wenn Daten ausschließlich für Zwecke der Statistik verarbeitet werden.
- Die Auswahl, Schulung von Erhebungsbeauftragten und ihr Einsatz in Wohnortnähe, sowie die Fragen des datenschutzgerechten Transports und der Aufbewahrung von Erhebungsunterlagen. Hier hatten wir auf

die Ausstattung der Erhebungsbeauftragten mit verschließbaren Aktenkoffern und die Verwendung von verplombten Umschlägen für die ausgefüllten Fragebögen gedrungen. Unserer Forderung wurde jedoch nicht nachgekommen.

- Kritisiert wurde durch die Datenschutzbeauftragten, dass einige Statistische Landesämter einzelne statistische Arbeiten, wie etwa die Digitalisierung der ausgefüllten Erhebungsbögen, an private Auftragnehmer vergeben haben. Statistische Kernarbeiten sind aus Gründen des Datenschutzes im abgeschotteten Bereich der amtlichen Statistik durchzuführen. Das Statistische Amt für Hamburg und Schleswig-Holstein ist dem nachgekommen. Hier wurden lediglich der Druck, die Personalisierung sowie der Versand und eine Vorabeingangsregistrierung der Fragebögen im Rahmen einer Auftragsdatenverarbeitung an private Dienstleister vergeben.

- Im Juni 2011 sind bei uns eine Vielzahl von Bürgereingaben eingegangen, welche ungerechtfertigte Erinnerungsschreiben des Statistischen Amtes an Hamburger und Schleswig-Holsteiner Bürger zum Gegenstand hatten. Tausende Bürger hatten Erinnerungsschreiben erhalten, obwohl sie ihrer Auskunftspflicht bereits nachgekommen waren. Betroffen waren sowohl Bürger, die die Fragebögen postalisch beantwortet hatten, als auch Bürger, die von der Möglichkeit der Online-Beantwortung Gebrauch gemacht hatten. Unmittelbar nach Bekanntwerden der Panne hatten wir das Statistische Amt hinsichtlich der Ursache und des Umfangs des Problems sowie zu der Frage, ob es zu einem Datenverlust gekommen ist, zur Stellungnahme aufgefordert. Als Ursache stellte sich schließlich heraus, dass für die Erinnerungen auf die Vorabeingangsregistrierung des Rücklaufs verschlossener Umschläge bei der Post abgestellt worden war. Wenn jedoch mehrere Auskunftspflichtige ihre Fragebögen in nur einem Umschlag oder nicht im Originalrückumschlag zurückgesandt hatten, wurden ihre Antworten nicht erfasst. Der Fehler bei der Online-Beantwortung war auf die mangelnde Anwenderfreundlichkeit der Software zurück zuführen. So war nicht klar ersichtlich, was zum Absenden zu tun ist, und es fehlte an einer Sendebestätigung. Diese Fehler wurden inzwischen behoben. Ein zunächst befürchteter Datenverlust konnte nicht festgestellt werden.

Wir werden die Durchführung des Zensus 2011 weiterhin kritisch begleiten. Dabei werden wir insbesondere darauf achten, dass die identifizierenden Hilfsmerkmale zum frühest möglichen Zeitpunkt gelöscht werden. Aus diesem Grunde haben wir ein Löschkonzept angefordert.

19.2 Landesinformationssystem (LIS)

Trotz bereits erfolgter Verbesserungen konnten unsere datenschutzrechtlichen Bedenken bislang noch nicht vollständig ausgeräumt werden.

Seit Februar 2010 sind wir mit der geplanten Einführung eines Landesinformationssystems (LIS) durch das Statistische Amt für Hamburg und Schleswig-Holstein befasst. Das Landesinformationssystem ist ein datenbankgestütztes, statistisches Informationssystem, welches die individuelle Auswertung von Statistikdaten mittels einer grafischen Benutzeroberfläche ermöglicht.

Das Statistische Amt für Hamburg und Schleswig-Holstein hat für das Landesinformationssystem drei Anwendungsbereiche vorgesehen, welche sich sowohl hinsichtlich des zugriffsberechtigten Personenkreises, der Zugriffswege, des Umfangs der Zugriffsrechte als auch der verfügbaren Auswertungsmöglichkeiten unterscheiden, jedoch grundsätzlich die gleiche Datenbasis nutzen sollen:

- Die „LIS-Kernanwendung“ dient der Bereitstellung aktueller statistischer Einzeldaten für die Fachanwender des Statistischen Amtes. Ein Zugriff auf die Daten/Dimensionen über die LIS-Kernanwendung ist nur innerhalb des Netzwerkes des Statistikamtes und nur für die Mitarbeiter des Statistikamtes im Rahmen ihrer fachlichen Aufgaben vorgesehen. Ad-hoc-Auswertungen sind hier ebenso möglich wie die Bereitstellung regelmäßig wiederkehrender Standard-Abfragen.
- Als „Extranet“ wird ein zweiter Anwendungsbereich bezeichnet, welcher ausgewählten Behörden und Ministerien in Hamburg und Schleswig-Holstein innerhalb des Landesnetzes den Zugang auf Teilbereiche des LIS-Datenbestandes über eine Terminalserverlösung ermöglicht. Der berechtigte „Extranet“-Nutzer soll über die LIS-Kernanwendung explizit bereitgestellte Datenquader sichten und alle Funktionen des LIS zur eigenen Datenauswertung nutzen können.
- Über die Internetanwendung „Infothek“ soll zudem auch dem statistikinteressierten Internetnutzer über eine Online-Datenbank nicht nur die Möglichkeit eröffnet werden, statistisch aufbereitete Ergebnistabellen einzusehen. Der Nutzer soll sich Ergebnisse auch selbst zusammen stellen und dynamisch erzeugen lassen können, wobei ein Zugriff nur auf einen definierten Teilbereich des replizierten Datenbestandes möglich ist.

Insbesondere bezüglich der geplanten Bereitstellung von Daten im „Extranet“ und in der „Infothek“ für eine Auswertungsmöglichkeit durch Dritte wurden von uns datenschutzrechtliche Bedenken geltend gemacht.

Im Rahmen von statistischen Erhebungen werden bei den Betroffenen vielfältige Einzelangaben über persönliche und sachliche Verhältnisse erhoben. Dies stellt einen Eingriff in die informationelle Selbstbestimmung dar. Bundes- und Landesstatistiken, bei denen Angaben über persönliche oder sachliche Verhältnisse erhoben werden und bei denen eine Auskunftspflicht besteht, müssen daher gesetzlich angeordnet werden. Die erhobenen Daten unterliegen zudem dem besonderen Schutz des Statistikgeheimnisses. Diese Geheimhaltungspflicht gilt bereits bei der Verarbeitung der Daten durch das Statistikamt, insbesondere jedoch bei der Bereitstellung von statistischen Daten für Dritte sowie der Veröffentlichung statistischer Ergebnisse. Hierbei muss stets gewährleistet sein, dass Einzelangaben den Betroffenen nicht zuzuordnen sind.

Da im geplanten Online-Verfahren dem interessierten Internet-Nutzer die Möglichkeit eröffnet werden soll, selbst Abfragen zu generieren, müssen die Einzeldatensätze vor der Übernahme in den für den Internet-Nutzer bereitgestellten Datenbestand statistisch zusammengefasst, d.h. aggregiert werden, um einen Rückbezug verlässlich auszuschließen. Darüber hinaus muss sichergestellt werden, dass auch aus dem Gesamtbestand der bereits aggregierten Daten kein Rückbezug, z. B. durch Subtraktion, herstellbar ist.

Unseren diesbezüglichen Anforderungen ist das Statistische Amt inzwischen dahingehend nachgekommen, dass für die „Infothek“ nur noch ein durch die Fachabteilungen freigegebener, selektiv replizierter Datenbestand bereit gestellt wird.

Zudem hat das Statistikamt inzwischen eine Erhebung nach BSI-Grundschutz für das Verfahren beauftragt.

Die Bereitstellung von statistischen Einzeldatensätzen für eigene Auswertungen Dritter, wie sie durch das Statistische Amt zunächst für die „Infothek“ und derzeit noch für den Bereich des „Extranet“ vorgesehen ist, geht über die Bereitstellung statistischer Ergebnisse hinaus und findet in den einschlägigen Statistikgesetzen keine Rechtsgrundlage.

19.3 Ankauf von soziodemographischen Daten durch Behörden

Die öffentliche Verwaltung unterliegt engen Bindungen, wenn sie statistische Daten von privaten Firmen kaufen und nutzen will.

Die Behörde für Schule und Berufsbildung beabsichtigte, bei einer privaten Firma statistisches Material anzukaufen, um daraus Rückschlüsse auf die Verteilung sozialer Bevölkerungsschichten im Verhältnis zum Bildungs-

niveau ziehen zu können. Dies führte im November 2010 zu einer öffentlichen Diskussion, in die wir eingebunden waren.

Kleingliedrige statistische Angaben, zum Teil heruntergebrochen bis auf Häuser und Häuserblöcke, gibt es inzwischen zu allen erdenklichen Fragestellungen mit Informationen über Lebensstandard, Interessen, Konsumverhalten, Gesundheitszustand, Wahlverhalten, Beschäftigung, Bildung etc.. Zusammengefasst werden diese als soziodemographische Daten bezeichnet, die von privaten Firmen zum Kauf angeboten werden. Derartige Daten lassen sich nicht nur für Kommunikations- und Werbemaßnahmen, sondern auch für Verwaltungszwecke verwenden. Beim Ankauf solcher Daten durch Behörden sind insbesondere die Belange des Datenschutzes zu berücksichtigen.

Die Anwendbarkeit des Datenschutzrechtes hängt davon ab, ob Informationen ein Personenbezug zukommt oder nicht. Zusammenfassende Angaben bzw. aggregierte Daten sind keine personenbezogenen Daten, es sei denn, einer Person kann eine Angabe zugeordnet werden. Eine Zusammenfassung liegt nur vor, wenn über die Verhältnisse der einzelnen Personen nichts mehr ausgesagt wird. Wann dies der Fall ist, hängt von Art, Menge, Detailliertheit und Kombinations- und Verschneidungsmöglichkeiten der Daten ab. Aggregierte Daten können auch dann personenbezogene Daten sein, wenn ein Gruppenergebnis im gegebenen sozialen Kontext den einzelnen Mitgliedern zugerechnet wird. Personenbezogene Daten liegen vor, wenn die Bezugsperson bestimmt, aber auch bereits dann, wenn die Bezugsperson nur bestimmbar ist. Letzteres ist der Fall, wenn die Person zwar nicht aus den Daten allein identifiziert, jedoch mit Hilfe anderer zusätzlicher Informationen festgestellt werden kann.

Statistische Angaben sind grundsätzlich nicht personenbezogen. Erst wenn die statistische Aussage einer konkreten Person zugeordnet wird, wird die bisherige statistische zur personenbezogenen Aussage. Dies ist der Fall, wenn Daten über die Wohnung oder das Wohnumfeld oder andere statistische Daten einer Wohnung und den darin lebenden Personen zuzuordnen sind. Auch Daten, die eine statistische Häufigkeit abbilden, können ab einer bestimmten Kleinräumigkeit personenbezogen sein. Kriterium ist, ob das untersuchte Milieu, für das statistische Wahrscheinlichkeiten erhoben werden, einen Rückschluss auf einzelne Individuen ermöglicht. Soweit Informationen sich auf die Charakteristika von individualisierbaren Haushalten beziehen (z. B. Sinus-Milieus), werden diese Bewertungen allen Mitgliedern in dem Haushalt zugeschrieben und müssen damit als personenbezogen (wenn auch nicht unbedingt als richtig) angesehen werden.

Soziodemographische Daten auf der Grundlage von georeferenzierten Profil- und Milieubildungen, bei denen es zunächst nur um die Zuordnung von Wahrscheinlichkeiten geht, können bei der Verknüpfung mit bestimmten Personen dennoch die Anwendung des Datenschutzrechts auslösen. Werden diese „weichen" Daten mit der Information gekoppelt, dass etwa eine bestimmte Person unter einer bestimmten Adresse wohnt, so werden die Durchschnittsangaben und Wahrscheinlichkeiten einer konkreten Person zugeordnet. Es liegt dann eine Erhebung bzw. Verarbeitung von personenbezogenen Daten vor, die einer Rechtgrundlage bedarf.

Die Art und Weise wie die Milieu- und Profilbildungen durch die Geomarketing-Firmen vorgenommen werden, kann die öffentliche Stelle nur schwer nachvollziehen. Dies gilt auch für die Frage, ob die der Milieu- und Profilbildung zugrundeliegende Datenerhebung durch die Geomarketing-Firmen datenschutzrechtlich korrekt war. Ein Rechtsverstoß würde hier unmittelbar auf die Verwaltung durchschlagen. Denn der Ankauf dieser Daten durch die öffentliche Stelle stellt insoweit eine Erhebung dar, für die es einer Rechtsgrundlage bedarf. Daher haben wir der Verwaltung empfohlen, in jedem Fall davon abzusehen, personenbezogenes statistisches Material zu kaufen. Die Behörde für Schule und Berufsbildung ist dieser Empfehlung im konkreten Fall gefolgt, zumal solchen Milieu- und Profilbildungen häufig ein hohes Diskriminierungspotenzial innewohnt.

Wir haben zu dieser Thematik eine Handreichung als Entscheidungshilfe für Behörden erstellt, die künftig als Leitfaden dienen kann. Sie ist auf unserer Homepage unter www.datenschutz-hamburg.de/datenschutz-fuer-firmen-behoerden/statistik abrufbar.

20. Rundfunk

20.1 Rundfunkbeitrag statt Rundfunkgebühr

Der Systemwechsel vom Geräte abhängigen zum Geräte unabhängigen Rundfunkbeitrag hat uns im Berichtszeitraum sehr beschäftigt. Leider wurde die Neuausrichtung nicht in ausreichendem Maße für ein datenschutzfreundlicheres Gebühreneinzugsverfahren genutzt.

Die Rundfunkfinanzierung soll auf eine neue Basis gestellt werden. Bisher knüpft die Pflicht zur Entrichtung von Rundfunkgebühren daran an, ob und welche Rundfunkempfangsgeräte eine Person besitzt. Zukünftig wird es nicht mehr nötig sein, Feststellungen darüber zu treffen, ob jemand nur ein Radio oder auch ein Fernsehgerät oder etwa einen Rundfunkempfangsfähigen Computer besitzt. Denn ab dem 1. Januar 2013 soll es gar nicht mehr darauf ankommen, ob eine Person überhaupt ein Gerät zum Emp-

fang von Radio- oder Fernsehprogrammen bereit hält, sondern jeder Haushalt und jeder Betrieb hat einen Rundfunkbeitrag zu entrichten. Dies sieht der neue Rundfunkbeitragsstaatsvertrag (RBStV) vor, der inzwischen Gesetzeskraft erlangt hat (Gesetz zum Fünfzehnten Rundfunkänderungsstaatsvertrag vom 15. Februar 2011, HmbGVBl. 2011, S. 63).

Wie auch die anderen Datenschutzbeauftragten der Länder, hatten wir gehofft, dass nun über die Beitragspflichtigen weniger Daten erhoben werden, weil keine Nachforschungen über den Besitz von Empfangsgeräten mehr erforderlich wären. Doch die Rundfunkanstalten haben, trotz guter Argumente der Landesdatenschutzbeauftragten, letztlich Regelungen entworfen, die teilweise zur Erhebung von mehr personenbezogenen Daten führen, als dies beim Gebührenmodell der Fall ist.

Im April 2010 erhielten die Datenschutzbeauftragten der Länder einen ersten Entwurf des neuen Staatsvertrags, der später die Bezeichnung „Rundfunkbeitragsstaatsvertrag“ (RBStV) erhielt. Die Landesdatenschutzbeauftragte des Landes Brandenburg in ihrer Funktion als Vorsitzende des Arbeitskreises Medien der Datenschutzbeauftragten übernahm es, die Stellungnahmen der Landesdatenschutzbeauftragten zu bündeln und gegenüber der Staatskanzlei Rheinland-Pfalz, den Rundfunkreferenten und Datenschutzbeauftragten der Rundfunkanstalten zu vertreten. An diesen Stellungnahmen sowie der Vielzahl kritischer Bewertungen der mehrmals geänderten Staatsvertragsentwürfe haben wir maßgeblich mitgewirkt und uns auch bemüht, durch Beratungen der Behörde für Kultur und Medien und mit Stellungnahmen zu Drucksachenentwürfen des Senats auf eine datenschutzfreundliche Regelung des Beitragseinzugs Einfluss zu nehmen.

Grundsätzliche Kritik übten wir daran, dass die RBStV-Entwürfe den rechtsstaatlichen Geboten der Normenklarheit und Verhältnismäßigkeit sowie der Datensparsamkeit und der Direkterhebung beim Betroffenen nicht entsprachen. Außerdem vertraten wir die Auffassung, dass der Einsatz von Rundfunkgebührenbeauftragten zur Beitragsermittlung verzichtbar wäre. Trotz des Modellwechsels zum wohnungsgebundenen Beitrag würde der Umfang der Datenerhebung massiv ausgeweitet, statt ihn zu reduzieren.

Hinsichtlich der Möglichkeit, sich von der Beitragspflicht befreien zu lassen oder eine Ermäßigung in Anspruch zu nehmen, ist im Staatsvertrag nach wie vor vorgesehen, dass mit dem Antrag Originalbescheide der Leistungsträger oder beglaubigte Kopien bei der GEZ (Gebühreneinzugszentrale, ein gemeinsames Rechenzentrum der Landesrundfunkanstalten) vorgelegt werden. Wir hatten vorgeschlagen, in der Norm zu regeln, dass

Leistungsbescheide nur dann verlangt werden dürfen, wenn sog. Drittbescheinigungen, in denen die Leistungsbehörde lediglich den Leistungsbezug und den Leistungszeitraum bescheinigt, von der Leistungsbehörde nicht ausgestellt werden. Bei Vorlage von Originalbescheiden bzw. deren beglaubigten Kopien sollten nach unserer Vorstellung nur die entscheidungserheblichen Daten von Hand in die EDV der GEZ aufgenommen und der Bescheid sodann zurück gesendet werden. Diese datensparsame Handhabung wurde mit dem Argument abgelehnt, der Personalaufwand bei der GEZ wäre dafür zu hoch; es bleibt also dabei, dass der Leistungsbescheid vollständig und ohne Schwärzung der nicht erforderlichen Daten bei der GEZ eingescannt wird.

Auch weitere vorgesehene Nachweispflichten sehen wir sehr kritisch. So ist der Beitragsschuldner verpflichtet, bei einer Abmeldung den „die Abmeldung begründenden Lebenssachverhalt“ mitzuteilen und auf Verlangen „nachzuweisen“. Nach dieser Formulierung wären nach unserer Ansicht besonders tief greifende Eingriffe in das Persönlichkeitsrecht des Beitragsschuldners möglich, beispielsweise eine Forderung, den Grund eines Wohnungswechsels mitzuteilen und ggf. ein Scheidungsurteil oder sonstige sehr persönliche Unterlagen vorzulegen.

Ebenfalls nicht durchsetzen konnten wir uns mit der Forderung, die Datenerhebung bei privaten Stellen auszuschließen. Wir können nicht erkennen, welchen zusätzlichen Erkenntnisgewinn diese Maßnahme bringen soll. Nach der sehr offenen Formulierung im RBStV dürften die Landesrundfunkanstalten Angaben z. B. von Arbeitgebern, Auskunfteien und dem Adresshandel einholen.

Teilweise Erfolg hatte die Kritik an der zunächst vorgesehenen Speicherdauer von nicht mehr benötigten Daten oder personenbezogenen Daten, deren Relevanz unklar ist. Erhobene Daten sind nunmehr unverzüglich zu löschen, wenn feststeht, dass sie nicht mehr benötigt werden oder eine Beitragspflicht dem Grunde nach nicht besteht; nicht überprüfte Daten sind spätestens nach 12 Monaten zu löschen.

Da dem neuen Rundfunkbeitragsrecht ein Staatsvertrag zwischen allen Ländern zugrunde liegt, gab es für Senat und Bürgerschaft nur eingeschränkte Möglichkeiten, eigene Regelungsvorstellungen durchzusetzen. Immerhin haben die Länder in Protokollerklärungen zum RBStV eine Evaluierung gefordert, mit der die Auswirkungen auf die Erträge aus dem Aufkommen des Rundfunkbeitrags angeht; es bleibt abzuwarten, ob es gelingt, die Evaluierung auf die Notwendigkeit der umfangreichen Datenerhebungsmöglichkeiten auszudehnen.

Inzwischen haben die Landesrundfunkanstalten Bereitschaft gezeigt, den RBStV unterhalb des Staatsvertrags durch Satzung und Verwaltungsvereinbarungen in datenschutzrechtlicher Hinsicht zu entschärfen. Dabei wird zu beobachten sein, ob damit untergesetzliche Regelungen geschaffen werden, die hinreichend klar sind, um bei späteren Änderungen des RBStV darin übernommen zu werden. Auch künftig werden die Landesdatenschutzbeauftragten bei Änderungen des RBStV versuchen, ihre Forderungen nach einem datenschutzgerechten Verfahren durchzusetzen.

IV. DATENSCHUTZ M NICHT-ÖFFENTLICHEN BEREICH

1. Videoüberwachung

1.1 Überblick

Die Anzahl von Beschwerden über eingesetzte Überwachungskameras ist weiter gestiegen. Verantwortliche Stellen kommen ihrer gegenüber der Datenschutzaufsichtsbehörde bestehenden Auskunftspflicht nur sehr zögerlich nach.

Unterschiedliche Kameratypen

Auch in diesem Berichtszeitraum haben sich wieder viele Bürgerinnen und Bürger an uns gewandt, weil sie sich durch installierte Überwachungskameras in ihrem Recht auf informationelle Selbstbestimmung verletzt fühlten. Die überwiegende Anzahl der Beschwerden hat sich gegen Überwachungen in Wohnanlagen und in Einzelhandelsgeschäften gerichtet. Aber auch die Videoüberwachung in nicht öffentlich zugänglichen Büroräumen erfolgte nach unserer Wahrnehmung in verstärktem Maße.

Sofern wir Zweifel an der Zulässigkeit der Videoüberwachung nach datenschutzrechtlichen Vorschriften haben, fordern wir die für die Videoüberwachung verantwortliche Stelle zu einer Stellungnahme auf und verlangen die Beantwortung eines Fragenkatalogs zur Videoüberwachung. Private Stellen und Privatpersonen sind nach § 38 Abs. 3 Bundesdatenschutzgesetz regelmäßig verpflichtet, der Datenschutzaufsichtsbehörde auf Verlangen die notwendigen Auskünfte unverzüglich zu erteilen.

Leider kommen viele Betreiber von Videoüberwachungsanlagen dieser Verpflichtung zur Auskunftserteilung trotz angemessener Fristen und mehrfacher Erinnerung nur zögerlich oder gar nicht nach. Die verantwortlichen Stellen lassen dabei außer Acht, dass dieses Verhalten ordnungswidrig ist und mit einer Geldbuße bis zu 50.000 Euro geahndet werden kann. Im Berichtszeitraum haben wir in zwei Fällen entsprechende Ordnungswidrigkeitsverfahren eingeleitet.

Die nachfolgend dargestellten Einzelfälle bieten einen guten Überblick der bearbeiteten Fälle und die vorgenommenen datenschutzrechtlichen Bewertungen. Sie können sowohl Bürgerinnen und Bürgern als auch verantwortlichen Stellen nützliche Hinweise liefern, ob eine bereits installierte oder eine geplante Videoüberwachungsanlage datenschutzrechtlich bedenklich oder unbedenklich ist.

1.2 Videoüberwachung in Einkaufszentren

Erfolg für den Datenschutz – ECE baut bundesweit Kameras in Ladenpassagen der Einkaufszentren ab.

Die Zulässigkeit der Videoüberwachung in den bundesweit von der Hamburger Gesellschaft ECE Projektmanagement GmbH & Co. KG (im folgenden ECE) betriebenen Einkaufszentren ist seit 2008 immer wieder Gegenstand von Erörterungen im Düsseldorfer Kreis gewesen. Die datenschutzrechtliche Problematik ist in unserem letzten Tätigkeitsbericht (22. TB, 1.3) ausführlich dargestellt worden. Während die in den Einkaufszentren auf Fluchtwege, Schließfächer, Kassenautomaten, Anlieferungszonen und Parkbereiche gerichteten Videokameras im Wesentlichen als zulässig erachtet wurden, bestanden gegen die großflächige Videoüberwachung in den Ladenpassagen – einschließlich der Ein- und Ausgänge, Verbindungen der Ladenstraßen, Eingänge zu einzelnen Geschäften und Rolltreppen – erhebliche datenschutzrechtliche Bedenken. Bei der Videoüberwachung der Ladenpassagen erfolgte keine unmittelbare Beobachtung der Videobilder durch Sicherheitspersonal. Die von den Kameras erfassten Bilder wurden in einem digitalen Ringspeicher, einer so genannten Black Box, gespeichert und nach 48 Stunden automatisch überschrieben, falls kein besonderer Vorfall Anlass zur Auswertung der Bilder gab.

Wegen des Unternehmenssitzes in Hamburg wurde im Düsseldorfer Kreis verabredet, dass wir in einem Musterverfahren gegen die Betreibergesellschaft eine Anordnung nach § 38 Abs. 5 BDSG wegen des Verstoßes bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten erlassen sollten. Die Anordnung erging im Dezember 2010 und bezog sich auf die Ladenpassage eines in Hamburg gelegenen Einkaufszentrums. Darin wurde der Abbau von 24 Videokameras mit der Begründung gefordert, dass die Videoüberwachung durch die auf die Ladenpassagen gerichteten Kameras nicht nach § 6b BDSG zur Wahrnehmung des Hausrechts oder der berechtigten Interessen der Betreibergesellschaft zulässig sei.

Im Einzelnen ist ausgeführt worden, dass die Befugnis der ECE, Ladenbesitzer in den Passagen vor in deren Geschäftsräumen begangenen

Straftaten schützen zu wollen, nicht von deren Hausrecht umfasst sei. Die Ladenbesitzer müssten ihr Eigentum selbst schützen, was auch durch in den einzelnen Geschäften installierte Videokameras geschehe. Das Hausrecht von ECE umfasse ebenfalls nicht das Recht zur allgemeinen Verhinderung von Straftaten in den Ladenpassagen, weil es sich nicht um Maßnahmen zum Schutz des Objektes oder zum Schutz eigener Rechtsgüter des Hausrechtsinhabers handele.

Grundsätzlich können zum Zweck der Wahrnehmung des Hausrechts Maßnahmen zur Verhinderung und nachträglichen Aufklärung von Beschädigungen in den Ladenpassagen, zur Verhinderung unzulässiger Prospektverteilung in der Passage sowie zur Durchsetzung der Hausordnung (z. B. der Einhaltung des Rauchverbots oder der Verhinderung unzulässiger Prospektverteilungen) erforderlich sein.

Allerdings ist die Videoaufzeichnung zur Verhinderung von Sachbeschädigungen und unzulässiger Prospektverteilung oder zur Durchsetzung des Rauchverbots nicht geeignet gewesen, da keine direkte Beobachtung, sondern nur eine nachträgliche Aufzeichnung erfolgte. Eine nachträgliche Auswertung bringt in diesen Fällen jedoch nichts. Die gewählte Form der Videoüberwachung als reine Aufzeichnungslösung („Black-Box“) ist nicht geeignet gewesen, einen präventiven Zweck zu erfüllen. Zur Straftatenprävention kann eine Videoüberwachung nur dann beitragen, wenn gerade durch eine Beobachtung im Sinne des. § 6b Abs.1 BDSG, also durch das Betrachten der Kamerabilder in Echtzeit mittels eines an sicherer Stelle betriebenen Bildausgabegerätes (Monitor), eine Intervention initiiert werden kann.

Auch für die Abwehr eines unberechtigten Betretens bzw. die Überwachung von bereits erteilten Hausverboten ist eine Black-Box-Lösung nicht geeignet. Zwar kann grundsätzlich auch die abschreckende Wirkung der Aufzeichnung durch eine Kamera mit der Möglichkeit der späteren Ermittlung der Täter, etwa durch staatliche Strafverfolgungsorgane, hinreichend sein, um die Rechtsposition des Hausrechtsberechtigten durchzusetzen. Bei unzulässigen Prospektverteilungen sowie Verstößen gegen das Rauchverbot handelt es sich jedoch um Bagatellverstöße, bei denen der Täter praktisch nicht mit der Verfolgung und der Auswertung der Videoaufzeichnung rechnet, so dass eine abschreckende Wirkung durch die bloße Existenz der Videoaufzeichnung nicht erreicht wird. Diese Einschätzung ist auch durch die von ECE zur Notwendigkeit der Videoüberwachung aufgeführten Vorkommnisse belegt worden. Die Aufstellungen von ECE haben gezeigt, dass in der Vergangenheit trotz erfolgter Videoüberwachung zum Beispiel nicht die in den Aufstellungen genannten Vorfälle der Misshaltung des Rauchverbots, der Belästigungen durch Spucken oder

das Versprühen von Tränengas verhindert werden konnten. Verhindert werden kann auf diese Weise auch nicht, dass Personen, denen gegenüber Hausverbote ausgesprochen wurden, nicht wieder ein Einkaufszentrum betreten. Dies kann nur durch eine Videoüberwachung als Monitorlösung sowie anwesendes Sicherheitspersonal geschehen.

Die nachträgliche Aufklärung von Beschädigungen in den Ladenpassagen durch Videoaufzeichnung unterfällt zwar ebenfalls dem Hausrecht von ECE. Die Auswertung von Videoaufzeichnungen ist zur Unterstützung bei der Täterermittlung und damit als repressive Maßnahme auch geeignet. Gegen die Erforderlichkeit spricht jedoch, dass die Täterermittlung auch mit anderen Maßnahmen, wie der Befragung von Zeugen, durchgeführt werden kann. Zudem war die Videoüberwachung für diesen Zweck auch nicht angemessen.

Denn die Betroffenheit von ECE war als eher gering anzusehen, da sich aus den von ECE übersandten Aufstellungen zu Vorkommnissen keine Anhaltspunkte für Sachbeschädigungen innerhalb der Ladenpassagen in einem nennenswerten Umfang ergeben haben. Erwähnt wurde mehrfach die Beschädigung von Mülleimern in der Mall. Es wurde nicht dargelegt und konnte daher auch nicht nachgeprüft werden, dass tatsächlich eine Gefahr von erheblichen Sachbeschädigungen bestanden hat.

Nach unserer Auffassung war die Videoüberwachung in den Ladenpassagen auch nicht zur Wahrnehmung berechtigter Interessen von ECE nach § 6b Abs. 1 Nr. 3 BDSG erforderlich und zulässig. Die allgemeine Verhinderung von Straftaten und die Erleichterung der Aufklärung von Straftaten in den Ladenstraßen wurden von uns nicht als ein berechtigtes Interesse von ECE im Sinne von § 6b Abs. 1 Nr. 3 BDSG anerkannt. Generalpräventive Maßnahmen und die Aufklärung von Straftaten sind in erster Linie öffentliche Aufgaben und obliegen daher dem Staat. Ebenso wie im öffentlichen Straßenraum ist es auch in den Einkaufszentren Sache der Besucher, auf sich und ihr Eigentum aufzupassen. Auch wenn eine gewisse Abschreckungswirkung von Videokameras ausgehen mag, ist zu berücksichtigen, dass im öffentlich zugänglichen Raum keine allgemeine Berechtigung des einzelnen Bürgers oder von Unternehmen besteht, überall dort, wo möglicherweise Straftaten vorkommen können, eine Videoüberwachung zu installieren.

Nach unserer Auffassung ist die Videoüberwachung der Ladenpassagen auch nicht zur Erfüllung von Verkehrssicherungspflichten durch ECE erforderlich gewesen, da mangels Monitoring eine sofortige Intervention von vornherein ausgeschlossen war. Zum Nachweis des Hergangs eines Schadensfalls ist die Videoaufzeichnung nicht erforderlich gewesen, da der Be-

weis, dass ein Schaden von ECE zu verantworten ist, von dem Anspruchsteller zu führen ist. Im Regressfall kann ein Entlastungsbeweis durch ECE auch auf andere Weise als durch die Auswertung von Videoaufzeichnungen geführt werden, zum Beispiel anhand eines lückenlosen Wartungsprotokolls der technischen Einrichtungen. Eine andere Betrachtungsweise hätte zudem die Konsequenz, dass überall dort, wo Verkehrssicherungspflichten bestehen, immer eine Videoüberwachung erforderlich wäre.

Bei Erlass der Anordnung sind wir davon ausgegangen, dass die Interessen der Besucher und Angestellten, nicht ständig im Einkaufszentrum von einer Videoüberwachung erfasst zu werden, die dargestellten Interessen von ECE überwiegen. Dies ergibt sich aus der Wertung des Rechts der Besucher und Angestellten auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts und der Menschenwürde. Das Recht auf informationelle Selbstbestimmung schließt das Recht des Einzelnen ein, sich in der Öffentlichkeit frei bewegen zu können, ohne befürchten zu müssen, ständig beobachtet zu werden. Besucher von Einkaufszentren können sich einer umfassenden und ständigen Videoüberwachung in den Ladenpassagen nicht entziehen und werden dadurch in ihren Rechten unangemessen beeinträchtigt. Dabei wurde berücksichtigt, dass die Betroffenheit der Besucher auch nicht dadurch gemindert wurde, dass es sich nur um eine Aufzeichnung in einer so genannten Black Box handelte. Durch den Schutzbereich der informationellen Selbstbestimmung soll der Betroffene nicht nur vor der übermäßigen Auswertung über ihn gespeicherter Daten geschützt werden, sondern bereits schon vor der übermäßigen Speicherung seiner personenbezogenen Daten. Die Interessenlage hatten wir bereits ausführlich im 22. TB 1.3 dargestellt.

ECE hat gegen die erlassene Anordnung Widerspruch eingelegt, der zurückgewiesen wurde. Daraufhin hat das Unternehmen im April 2011 erklärt, dass die Geschäftsführung der ECE zu der Auffassung gelangt sei, dass auf die beanstandeten Kameras verzichtet werden könne und diese abgebaut würden. Außerdem hat das Unternehmen erklärt, dass entsprechende Kameras auch in den Ladenpassagen der anderen deutschen Einkaufszentren des Unternehmens abgebaut werden würden. Wir haben diese Entscheidung als datenschutzkonform und kundenfreundlich begrüßt und hoffen, dass damit deutschlandweit eine Signalwirkung auch für die Videoüberwachung in den Einkaufszentren anderer Betreiber entsteht.

Im Sommer 2011 hat der Konzerndatenschutzbeauftragte von ECE in einer mit uns abgestimmten Arbeitsanweisung die nationalen Center Manager zum Abbau der Videokameras in den Ladenpassagen aufgefordert. Der Abbau wurde mittlerweile in die Wege geleitet.

1.3 Videoüberwachung in Kassenbereichen

Einzelhändler nutzen vermehrt Kassentische, in die eine Kamera zur Überwachung der Einkaufswagen integriert ist. Dabei geraten auch Kunden in den Erfassungsbereich der Kameras.

Kamerasituationen im Kassenbereich

Durch eine Beschwerde wurden wir auf ein Einzelhandelsgeschäft aufmerksam, das seine Kassentische mit Kameras ausgestattet hatte. Die Kameras befanden sich in einer kleinen Öffnung an der Seite der Kassentische und waren etwa in Kniehöhe eingebaut. Neben den Kassen war ein kleiner Monitor für die Kassiererinnen und Kassierer installiert.

Nach Angaben der Verantwortlichen sollten die Kameras die Arbeit der Kassiererinnen und Kassierer erleichtern. Diese könnten durch einen Blick auf den Monitor ohne Aufstehen und ohne einen Blick in den an der Decke montierten Spiegel zu werfen feststellen, ob der Einkaufswagen tatsächlich leer sei. So könne sichergestellt werden, dass die Kassiererinnen und Kassierer alle Waren verbuchen können, auch wenn sie – bewusst oder unbewusst – im Einkaufswagen verblieben seien.

Unsere Überprüfung vor Ort ergab, dass nicht nur die Einkaufswagen in den Erfassungsbereich der Kamera gelangten. Sofern kein Einkaufswagen

direkt vor der Kameraöffnung abgestellt war, bildete die Kamera eine vor der Kasse stehende Person – je nach Körpergröße – von den Füßen bis zur Schritthöhe ab. Kleinere Kinder wurden von den Kameras vollständig erfasst. Aufgrund des weiten Winkels der Kameras wurden auch Personen, die sich an der gegenüberliegenden Kasse befanden und Personen, die sich in der Nähe des Eingangs- bzw. Ausgangs aufhielten, um dort z. B. Ihre Einkäufe zu verstauen, von den Kameras aufgenommen.

Nach § 6b BDSG ist eine Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Wir halten eine derartige Videoüberwachung für nicht für erforderlich, da der Überwachungszweck auch mit milderen Mitteln erreicht werden kann, die einen geringeren Eingriff in das informationelle Selbstbestimmungsrecht der von der Überwachung betroffenen Personen bewirken. Durch große, über allen Kassenbereichen installierte Spiegel wird es den Kassiererinnen und Kassierern in ausreichendem Maße ermöglicht, einen Blick in den Einkaufswagen zu nehmen. Darüber hinaus halten wir es für zumutbar, dass Kassiererinnen und Kassierer in „Verdachtsfällen“ kurz aufstehen, um den Einkaufswagen einzusehen oder Kunden bitten, ihre Taschen anzuheben.

Selbst wenn eine Erforderlichkeit der Videoüberwachung angenommen werden würde, stünden dem Interesse des Einzelhändlers, Vermögensschäden durch Diebstähle o.ä. zu verhindern, die schutzwürdigen Interessen der Kunden, in diesem Bereich nicht Gegenstand einer Videoüberwachung zu werden, entgegen.

Die Positionierung der Kameras in den Kassentischen, die Personen je nach Körpergröße bis zur „Schritthöhe“ erfassen, kann die Intimsphäre einzelner Kunden verletzen und ist daher nicht hinzunehmen. Zudem erfassen die Kameras in der vorgefundenen Ausrichtung auch Personen in Bereichen neben bzw. hinter den Kassen, für deren Überwachung – vor oder nach dem Einkauf – keine Veranlassung besteht.

Wir haben den Einzelhändler daher aufgefordert, diese nicht zulässige Videoüberwachung einzustellen. Dieser Aufforderung ist der Einzelhändler nachgekommen.

1.4 Videoüberwachung von Beschäftigten einer internationalen Unternehmensgruppe

Auch in deutschenTochterunternehmen internationaler Konzerne sind die Regelungen des Bundesdatenschutzgesetzes zu beachten. In diesem Fall hat das Unternehmen unmittelbar auf unsere datenschutzrechtlichen Einwände reagiert.

Bereits in unserem 21. Tätigkeitsbericht haben wir darüber berichtet, dass Arbeitgeber Videotechnik ohne vorherige Zulässigkeitsprüfung einsetzen. Diese Tendenz hat sich fortgesetzt.

Wir haben u. a. einen Hinweis auf eine Videoüberwachung von Büroräumen eines in Hamburg ansässigen Unternehmens erhalten. Dieses hamburgische Unternehmen gehört ebenso wie ein weiteres Unternehmen in Frankfurt am Main zu einer internationalen Unternehmensgruppe mit Sitz in Südkorea.

In den Büroräumen der Mutter- und Tochterunternehmen waren Videokameras installiert. Die Bilder der Videokameras konnten weltweit von allen Führungskräften und Mitarbeitern der Unternehmensgruppe jederzeit über das Internet oder Intranet aufgerufen werden. Mitarbeitern in Südkorea war es so möglich, ihre Kollegen in Hamburg und Frankfurt bei der Arbeit zu beobachten.

Als Erlaubnistatbestände einer Videoüberwachung von Beschäftigten in nicht öffentlich zugänglichen Räumen kommen § 28 Abs. 1 Nr. 2 und § 32 Abs. 1 BDSG unter Berücksichtigung der Rechtsprechung des Bundesarbeitsgerichtes in Betracht. Nach der Rechtsprechung des Bundesarbeitsgerichtes steht der Zulässigkeit einer dauerhaften verdachtsunabhängigen Videoüberwachung regelmäßig ein überwiegendes schutzwürdiges Interesse der Beschäftigten entgegen. Lediglich in Einzelfällen, bei konkretem Verdacht einer strafbaren Handlung, kann eine zeitlich begrenzte Videoüberwachung der Beschäftigten zulässig sein, wenn dies das einzig verbliebene Mittel zur Aufklärung ist.

Das hamburgische Unternehmen kam unserer Bitte um Stellungnahme zu der Videoüberwachung umgehend nach. Ein Rechtsanwalt des Unternehmens teilte mit, dass die Kameras installiert worden seien, um Videokonferenzen zwischen den verschiedenen Standorten der Unternehmensgruppe zu ermöglichen. Das Unternehmen habe nach einer datenschutzrechtlichen Beratung durch den Anwalt zwischenzeitlich alle Kameras in den Büroräumen der Standorte Frankfurt und Hamburg entfernt und werde zukünftig nur einen Besprechungsraum für Videokonferenzen nutzen.

Aufgrund der unmittelbaren Kooperationsbereitschaft und Einsichtigkeit der verantwortlichen Stelle haben wir auf weitere Maßnahmen gegen das Unternehmen verzichtet.

1.5 Videoüberwachung einer Zufahrtsschranke

Die Videoüberwachung einer Wohnanlagenzufahrt ist ein schwerwiegender Eingriff in das informationelle Selbstbestimmungsrecht der Bewohner und Besucher, da diese nicht die Möglichkeit haben, sich der Überwachung in diesem Übergang zum privaten Lebensbereich zu entziehen.

Deaktivierte Videoüberwachungsanlage

Uns erreichen weiterhin viele Beschwerden, die sich gegen Videoüberwachungen in Wohnanlagen (vgl. 21. TB) richten. In einem Fall haben uns Bewohner der Insel Sylt darüber informiert, dass die Zufahrtsschranke zu ihrer Wohnanlage videoüberwacht werde.

Da die Wohnanlage von einem in Hamburg ansässigen Unternehmen verwaltet wird, haben wir eine Überprüfung der datenschutzrechtlichen Zulässigkeit der Videoüberwachung vorgenommen.

In einer Stellungnahme hat das Unternehmen die Erforderlichkeit der Videoüberwachung mit möglichen Beschädigungen der Schranke begründet. Der Kreis Nordfriesland habe aufgrund massiver Probleme durch Falschparker (z. B. versperrte Rettungswege) den Einbau der Schranke verfügt. Dieser Einbau habe für erheblichen Unmut bei den Bewohnern ge-

sorgt. Aufgrund dessen sei davon auszugehen, dass die Schranke beschädigt werde.

Eine Überprüfung des zur Verfügung gestellten Überwachungsbildes ergab, dass die Kamera nicht nur den unmittelbaren Bereich der Schranke, sondern auch dahinter liegende öffentliche Straßen und Wege erfasste. Somit sind Bewohner, Besucher, Spaziergänger und vorbeifahrende Autos beobachtet und aufgezeichnet worden.

Eine Videoüberwachung ist nach den Vorschriften des BDSG unter Beachtung einer strikten Zweckbindung nur zulässig, soweit sie erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Die Erforderlichkeit der Videoüberwachung konnte uns das Unternehmen nicht belegen. Die bloße Vermutung, die Zufahrtsschranke könnte aufgrund des Unmutes der Bewohner beschädigt werden, haben wir nicht als eine ausreichende Begründung für die Erforderlichkeit einer Videoüberwachung dieses Bereiches akzeptiert.

Die Zulässigkeit der Videoüberwachung scheiterte darüber hinaus an den überwiegenden schutzwürdigen Interessen der Bewohner und Besucher. Eine Videoüberwachung der Zufahrtsschranke zur Wohnanlage ist ein schwerwiegender Eingriff in das informationelle Selbstbestimmungsrecht der betroffenen Personen, da es für diese nicht möglich ist, sich der Überwachung in diesem Übergang zum privaten Lebensbereich zu entziehen. Durch eine solche Videoüberwachung wird nicht nur jede Ankunft bzw. Abreise der Bewohner, sondern auch eventueller Begleitpersonen erfasst, so dass ein Einblick in das Privatleben der Bewohner möglich ist.

Wir haben das Unternehmen daher aufgefordert, die Kamera außer Betrieb zu setzen. Dieser Aufforderung ist das Unternehmen nachgekommen.

1.6 Kameraattrappen in einer Seniorenwohnanlage

Auch Kameraattrappen können einen Überwachungsdruck erzeugen und die Betroffenen zu Verhaltensänderungen veranlassen. Die Vorschriften des Bundesdatenschutzgesetzes greifen im Falle von Attrappen nicht. Unter Umständen besteht jedoch ein zivilrechtlicher Abwehr- und Unterlassungsanspruch.

Kameraattrappe in Seniorenwohnanlage

Im Berichtszeitraum hat uns die Beschwerde des Bewohners einer Seniorenwohnanlage erreicht. Die Vermieter hatten zur Überwachung der Flure der mehrgeschossigen Wohnanlage augenscheinlich 32 Videokameras installiert.

Wir haben die Vermieter zu einer Stellungnahme aufgefordert, da wir erhebliche Zweifel an der Zulässigkeit der Videoüberwachung hatten. Die Vermieter teilten uns mit, dass es sich bei den Kameras um Attrappen handelte, die der Abschreckung von Dieben dienen sollten. Aus den Fluren der Wohnanlage seien in der Vergangenheit einzelne Gegenstände entwendet worden, die die Bewohner dort vor oder neben ihren Wohnungen platziert hätten.

Bei einer Überprüfung vor Ort haben wir uns den Kaufbeleg mit der Produktbezeichnung der Kameras vorlegen lassen und eine Kamera zu Kontrollzwecken aus der Wand entfernt. Dabei hat sich herausgestellt, dass es sich tatsächlich um Kameraattrappen handelte.

Im Falle von Attrappen sind die einschlägigen Vorschriften des Bundesdatenschutzgesetzes nicht anwendbar. Attrappen ermöglichen weder eine Beobachtung noch handelt es sich bei ihnen um optisch-elektronische Einrichtungen. Sie können auch nicht zur Erhebung und Verarbeitung personenbezogener Daten genutzt werden. Diese Rechtslage empfinden wir als sehr unbefriedigend, da für den unbefangenen Beobachter die Funktionsunfähigkeit der Kameras nicht erkennbar ist. Auch Attrappen können somit einen Überwachungsdruck erzeugen und die Betroffenen zu Verhaltensänderungen veranlassen.

Wir haben dem Beschwerdeführer mitgeteilt, dass wir auf der Grundlage des Bundesdatenschutzgesetzes keine Maßnahmen gegen die vermeintliche Überwachung ergreifen können.

Die Installation der Kameraattrappen stellt dennoch einen Eingriff in das allgemeine Persönlichkeitsrecht des Bewohners dar, so dass ihm die Möglichkeit offensteht, einen Abbau der Kameras auf zivilrechtlichem Wege durchzusetzen. Von dieser Möglichkeit hat der Petent Gebrauch gemacht. Seine Klage hat jedoch in der ersten Instanz vor dem Amtsgericht Hamburg keinen Erfolg gehabt. Der zuständige Amtsrichter verneinte das Bestehen eines Überwachungs- und Anpassungsdrucks, da dem Kläger zwischenzeitlich bekannt sei, dass es sich um Attrappen handele und der Eingriff in die Individualsphäre des Klägers unter Berücksichtigung der Umstände dieses Einzelfalls gerechtfertigt sei.

Der Petent hat gegen dieses Urteil Berufung eingelegt. Wir werden über den Fortgang des Verfahrens berichten.

1.7 Videoüberwachung in Taxis

Eine Videoüberwachung in Taxis kann in sehr engen Grenzen zulässig sein.

Im Berichtszeitraum haben uns mehrere Beschwerden und Anfragen zur Videoüberwachung in Taxis erreicht. Auf Initiative Nordrhein-Westfalens hat sich auch der Düsseldorfer Kreis mit der Frage der Zulässigkeit einer Videoüberwachung in Taxis befasst.

Zwischen den Datenschutzaufsichtsbehörden der Länder besteht weitgehend Einvernehmen darüber, dass eine Videoüberwachung in Taxis zur Abwehr von Gefahren für Leben, Gesundheit und Freiheit der Taxifahrer in sehr engen Grenzen in Betracht kommen kann. Eine an diesen Zwecken orientierte Videoüberwachung muss nach § 6b BDSG erforderlich und verhältnismäßig sein.

Taxi-Unternehmer müssen insbesondere vor einer Installation von Kameras in ihren Taxis den Einsatz und die Realisierung alternativer Schutzvorkehrungen prüfen, die weniger tief in das informationelle Selbstbestimmungsrecht der Fahrgäste eingreifen. Beispielhaft zu nennen sind der Betrieb von Alarmsystemen und die Deponierung der Einnahmen in Sicherheitsfächern.

Sollte die Videoüberwachung des Fahrgastraumes trotz Realisierung anderer Schutzvorkehrungen alternativlos sein, sind bei der Ausgestaltung die folgenden Voraussetzungen einer zulässigen Videoüberwachung zu beachten:

- Keine permanente Aufzeichnung während der Fahrt. Zulässig sind die Aufnahme einzelner Standbilder oder die Aufzeichnung einer kurzen Videosequenz (ca. 15 Sekunden) beim Einstieg der Fahrgäste und eine Aktivierung der Kamera in Notfällen.

- Eine maximal 48-stündige Speicherung des Bildmaterials. Im Regelfall Löschung der Aufzeichnungen nach Schichtende.
- Hinweisschilder an den Fahrgasttüren und Nennung der verantwortlichen Stelle.
- Umsetzung von technischen und organisatorischen Maßnahmen, die gewährleisten, dass nur berechtigte Personen auf das Bildmaterial zugreifen können und somit ein unbefugtes Auslesen der Daten ausgeschlossen ist.
- Erstellung einer Verfahrensbeschreibung, Beachtung der Rechte der Betroffenen.

Unser Ziel ist es, diesen Rahmen einer zulässigen Videoüberwachung in Taxis in den nächsten Wochen und Monaten einer möglichst großen Zahl von Taxi-Unternehmern auf effektive und effiziente Weise zu vermitteln sowie die Einhaltung dieses Rahmens sicherzustellen.

Ein mögliches Informationsmedium für Taxi-Unternehmer sind die als Vermittler zwischen Fahrgast und Taxi-Unternehmer auftretenden Taxi-Funkzentralen. Vertreter einer großen hamburgischen Taxifunk-Zentrale haben uns in einem ersten Gespräch unmittelbar ihre Bereitschaft erklärt, gegenüber den verantwortlichen Taxi-Unternehmen als Multiplikator unserer datenschutzrechtlichen Anforderungen zu fungieren.

Im Verlauf des Jahres 2012 werden wir zudem bei einzelnen Taxi-Unternehmern, die eine Videoüberwachung einsetzen, datenschutzrechtliche Kontrollen durchführen.

1.8 Videoüberwachung im Apple Store Hamburg, Jungfernstieg

Auf den Umstand einer Videoüberwachung und die hierfür verantwortliche Stelle ist in geeigneter Form hinzuweisen – an sich eine Selbstverständlichkeit. Dieser Hinweispflicht wird im Apple Store Hamburg am Jungfernstieg trotz wiederholter Aufforderung noch nicht ausreichend nachgekommen.

Die Verpflichtung, auf eine Videoüberwachung hinzuweisen, ist Gegenstand des § 6b Abs. 2 BDSG. Dort heißt es, dass der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen sind. Die Hinweise sind deutlich sichtbar anzubringen. Was deutlich sichtbar ist, hängt von der Größe und Gestaltung des Hinweises, aber auch vom Umfeld und dem Hintergrund ab. Die optische Gestaltung und räumliche Anordnung des Hinweises ist so vorzunehmen, dass der Hinweis bereits vor dem Betreten des überwachten Bereiches erkennbar ist und sich im normalen Blickwinkel befindet, also nicht erst gesucht wer-

den muss. Dieser Regelung wird in vielen Fällen nicht oder nicht ausreichend Beachtung geschenkt.

So sind wir durch eine Bürgerbeschwerde u. a. auf die umfängliche, aber nicht kenntlich gemachte Videoüberwachung im Apple Store am Jungfernstieg aufmerksam geworden. Wir haben wegen dieses Mangels Kontakt mit der verantwortlichen Apple Retail Germany GmbH aufgenommen und auf die Verpflichtung zur Kenntlichmachung der Videoüberwachung hingewiesen. Leider genügen die zwischenzeitlich aufgestellten Hinweisschilder im Apple Store Jungfernstieg unseren Anforderungen immer noch nicht, da sie mit Blick auf die örtlichen Gegebenheiten zu klein sind und ihre Positionierung es den Kunden nicht ermöglicht, vor Betreten des überwachten Bereiches auf die Videoüberwachung aufmerksam zu werden.

Wir haben daher erneut Kontakt mit dem Unternehmen aufgenommen und gehen davon aus, dass unsere Anforderungen an eine datenschutzkonforme Kenntlichmachung der Videoüberwachung nunmehr zügig umgesetzt werden. Denn wie bereits erläutert (vgl. 1.4), gelten für Unternehmen eines Konzerns, die in Deutschland einer Verkaufstätigkeit nachgehen, die Regelungen des § 6b BDSG, auch wenn sich der Hauptsitz des Konzerns außerhalb der EU befindet.

Anzumerken ist, dass wir in diesem Fall nur in Amtshilfe für die hessische Datenschutzaufsichtsbehörde tätig geworden sind, da sich die Zuständigkeit der Datenschutzaufsichtsbehörden nach dem Sitz des betroffenen Unternehmens richtet. Diese Zuständigkeitsregelung soll sicherstellen, dass in einem Unternehmen einheitliche Datenschutzstandards etabliert werden.

1.9 Aufzeichnung von Telefongesprächen in Einkaufszentren

Aufzeichnungen von Telefongesprächen sind ohne Einwilligung der Anrufenden grundsätzlich unzulässig.

Im März 2011 haben wir einen Hinweis erhalten, dass in den von dem Hamburger Unternehmen ECE betriebenen Einkaufszentren eingehende Telefongespräche ohne einen Hinweis auf die Aufzeichnung gespeichert werden. Unsere Überprüfung hat ergeben, dass in allen von ECE in Hamburg betriebenen Einkaufszentren die beim Centermanagement unter der zentralen Rufnummer eingehenden Anrufe für eine Dauer von 48 Stunden gespeichert wurden mit der Begründung, Drohanrufe festhalten zu können. Gespeichert wurde auf digitalen Geräten, auf denen die Aufzeichnungen nach 48 Stunden überschrieben wurden. Auch der Landesdatenschutzbeauftragte Sachsen hat eine entsprechende Prüfung bei einem in Sachsen belegenen, von ECE betriebenen Einkaufszentrum durchgeführt.

Die Praxis des Unternehmens, jeden in der Zentrale des Center-Managements eingehenden Anruf für 48 Stunden aufzuzeichnen, stellt eine unbefugte Aufnahme des nichtöffentlich gesprochenen Worts eines anderen auf einen Tonträger dar, was nach § 201 Strafgesetzbuch (StGB) strafbar ist. Nach § 205 Abs. 1 StGB wird die Tat jedoch nur auf Antrag des Verletzten verfolgt.

Das Unternehmen hat unmittelbar nach Bekanntwerden der Vorwürfe veranlasst, dass in allen Einkaufszentren die Telefonaufzeichnungen gestoppt und die entsprechenden Geräte deinstalliert werden.

2. Internationaler Datenverkehr

2.1 Safe Harbor-Regelungen

Die Eintragung eines Unternehmens in die Safe-Harbor-Liste allein ist keine Gewähr für datenschutzrechtliche Sicherheit.

In den vergangenen Tätigkeitsberichten haben wir bereits mehrfach die Safe-Harbor-Regelungen angesprochen (20. TB, 18.2; 21. TB, 20.3). Dabei handelt es sich um ein Abkommen zwischen der EU und den USA, das es europäischen Unternehmen ermöglicht, personenbezogene Daten legal in die USA zu übermitteln. Nach den Vorschriften des Bundesdatenschutzgesetzes (BDSG) ist es nur unter besonderen Voraussetzungen zulässig, solche Daten in sogenannte Drittländer außerhalb der EU zu übermitteln (vgl. hierzu auch 19. TB, 19.2). Neben den bereits gesetzlich vorgesehenen zulässigen Datenübermittlungen gibt es nach dem BDSG auch die Möglichkeit, an Unternehmen in Drittländern Übermittlungen vorzunehmen, die entweder ein angemessenes Datenschutzniveau gewährleisten oder ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts vorweisen können.

Vor dem Hintergrund, dass die USA keine umfassenden gesetzlichen Regelungen kennen, die den Standards der EU-Richtlinie entsprechen, hat die EU im Jahr 2000 anerkannt, dass bei den Unternehmen, die dem Safe-Harbor-System beigetreten sind, ein angemessenes Datenschutzniveau besteht. An US-Unternehmen, die Safe Harbor beigetreten und auf der entsprechenden Liste des US-Handelsministeriums eingetragen sind, können europäische Unternehmen personenbezogene Daten erleichtert übermitteln, vorausgesetzt, dass die übrigen datenschutzrechtlichen Vorschriften eingehalten werden. Diejenigen Unternehmen, die in den USA dem Safe-HarborSystem beitreten, verpflichten sich, die Safe Harbor Principles und die dazugehörenden – verbindlichen – Frequently Asked Questions (FAQ) zu beachten. Die Liste der beigetretenen Unternehmen ist im Internet unter *https://safeharbor.export.gov/list.aspx abrufbar.*

Eine australische Studie aus dem Jahre 2008 hat aufgedeckt, dass erhebliche Mängel hinsichtlich der Richtigkeit der Liste, aber auch hinsichtlich der Einhaltung der Safe Harbor-Regelungen durch die eingetragenen Unternehmen bestehen. Insbesondere entsprechen die auf der Liste aufgeführten Unternehmen nicht dem aktuellen Stand, zumal die Zertifizierung regelmäßig erneuert werden muss.

Im Rahmen der zwischen der Art. 29 Datenschutzgruppe der EU und dem amerikanischen Handelsministerium regelmäßig stattfindenden Konferenzen über das Safe Harbor-System ist deutlich geworden, dass eine systematische Kontrolle der in der Safe Harbor-Liste registrierten Unternehmen durch die zuständige US-Aufsichtsbehörde Federal Trade Commission (FTC) nicht stattfindet. Immerhin geht das US-Handelsministerium jetzt gegen bekannt gewordene Verstöße vor und leitet entsprechende Verfahren ein.

Angesichts dieser Missstände im Hinblick auf die Verlässlichkeit der Liste hat der Düsseldorfer Kreis in seiner Sitzung im April 2010 einen Beschluss erlassen, der unter *https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2010/Pruefung_der_Selbst-Zertifizierung_des_Datenimporteuers/Beschluss_28_29_04_10neu.pdf* abrufbar ist. Die darin aufgeführte Verpflichtung für Daten exportierende Unternehmen, sich nachweisen zu lassen, dass die Safe Harbor-Selbstzertifizierung vorliegt und deren Grundsätze auch eingehalten werden, soll sicher stellen, dass die für die Datenverarbeitung verantwortlichen Stellen in Deutschland eine gewisse Kontrolle ausüben und sich nicht allein auf die Angaben in der Safe Harbor-Liste verlassen. Mindestens muss das exportierende Unternehmen klären, ob die Zertifizierung des amerikanischen Unternehmens noch gültig ist.

2.2 Fluggastdatenübermittlung

Die bisher vorliegenden Abkommen und Entwürfe zu Fluggastdatenübermittlungen begegnen nach wie vor datenschutzrechtlichen Bedenken.

In den vergangenen Jahren hat es mehrere Abkommen über die Übermittlung von Flugpassagierdaten auf internationaler Ebene (USA, Kanada, Australien) gegeben. Gleichzeitig haben auch im europäischen Raum die Begehrlichkeiten nach diesen Daten zugenommen (vgl. 21. TB, 20.1; 22. TB, IV 2.1).

Die Abkommen mit den USA und Australien mussten wegen des Zustimmungserfordernisses des Europäischen Parlaments neu ausgehandelt werden. Seit Mai 2011 gibt es eine Einigung zwischen der EU-Kommission

und Australien über ein neues Abkommen. Wegen fortbestehender Bedenken hinsichtlich der Rechtsgrundlage, der Laufzeitbeschränkung und der Speicherfrist stehen der Beschluss des Rates und die Unterzeichnung des Abkommens jedoch noch aus. Nach Verhandlungen mit den USA gibt es bereits seit Mai 2011 einen Abkommensentwurf, dieser warf zunächst nach Auffassung der Kommission weiteren Diskussionsbedarf auch angesichts datenschutzrechtlicher Bedenken auf. Im November 2011 hat die EU das Abkommen mit den USA jedoch vorläufig unterzeichnet, nach Zustimmung der EU-Innenminister – bei Enthaltung Deutschlands – im Dezember 2011 muss jetzt noch das EU-Parlament zustimmen. Einen neuen Entwurf für ein Abkommen mit Kanada gibt es bisher noch nicht. Die entsprechenden Verhandlungen wurden unterbrochen.

Anfang des Jahres 2011 hat die Europäische Kommission einen Vorschlag für eine „Richtlinie über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität“ eingebracht. Ein Beschluss des Bundesrates hierzu (Drucksache 73/11) bringt zum Ausdruck, dass der Richtlinienvorschlag das Gleichgewicht zwischen der Wahrung der Freiheitsrechte und dem Schutz der öffentlichen Sicherheit nicht in angemessener Weise herzustellen vermag. In dem mehrseitigen Papier werden die verfassungs- und datenschutzrechtlichen Bedenken unter verschiedenen Gesichtspunkten erläutert. Kritisiert werden insbesondere die anlasslose Speicherung, die fehlenden Ausführungen zur Erforderlichkeit der Erhebung der Daten, die vorgesehene lange Speicherfrist von fünf Jahren und einem Monat sowie die fehlende Rechtssicherheit für die Betroffenen.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich auf unsere Initiative mit dem Entwurf befasst und ihn in deutlicher Form kritisiert. Die Einzelheiten dazu können einem Entschließungsentwurf vom März 2011 unter http://www.datenschutz-bayern.de/dsbk-ent/DSK_81-Fluggastdaten.html entnommen werden. Die Beratungen über den Richtlinienentwurf werden voraussichtlich auch im Jahre 2012 noch andauern.

3. Telemedien

3.1 Anwendbares Recht und aufsichtsbehördliche Zuständigkeit bezüglich Facebook

Die Aufsichtsbehörden der einzelnen Länder der Bundesrepublik Deutschland sind zuständig für die Kontrolle der Einhaltung des deutschen Datenschutzrechts durch das soziale Netzwerk Facebook.

Facebook hat in den vergangenen Jahren einen ganz erheblichen Zulauf an Nutzern verzeichnen können. Leider sind wir immer wieder mit Eingaben und Vorwürfen befasst worden, die sowohl auf intransparente Datenschutz- und Nutzungsbestimmungen, aber auch auf die vielen Dienste, die Facebook den Nutzern anbietet, zurückgehen. Zur Klärung der Frage unserer Zuständigkeit und des anwendbaren Rechts haben wir ein Rechtsgutachten gefertigt, das wir der Art. 29-Gruppe in Brüssel zur weiterführenden Diskussion auf EU-Ebene mitgeteilt haben. In dem Gutachten, das abrufbar ist auf der Internet-Seite des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit *(www.datenschutz-hamburg.de/fileadmin/user_upload/documents/Gutachten_Facebook-Gesichtserkennung.pdf)*, gelangen wir zu dem Ergebnis, dass deutsches Datenschutzrecht anwendbar ist und die Aufsichtsbehörden der deutschen Bundesländer für die Datenschutzkontrolle zuständig sind.

Entgegen der seitens Facebook vertretenen Auffassung ist die Facebook Inc., USA die verantwortliche Stelle für die Tätigkeit des Dienstes. Dieses hat zur Folge, dass für die Facebook-Nutzer in Deutschland deutsches Datenschutzrecht anwendbar ist. Durch den Betrieb seines sozialen Netzwerkes verarbeitet und erhebt Facebook Daten in Deutschland (und jedem anderen EU-Mitgliedsstaat) indem es Cookies auf den Rechnern der Facebook-Nutzer ablegt.

Facebook behauptet demgegenüber, die Facebook Inc. verarbeite lediglich im Rahmen einer Auftragsdatenverarbeitung für Facebook Ireland Ltd. die Daten von Nutzern in Europa auf Servern in den Vereinigten Staaten. Dieses hätte zur Folge, dass irisches Datenschutzrecht für die gesamte EU auf Facebook – nämlich auf Facebook Ireland Ltd. – anzuwenden wäre.

Das ist unseres Erachtens jedoch nicht der Fall. Eine Auftragsdatenverarbeitung liegt nur dann vor, wenn die beauftragte Stelle – nach Auffassung von Facebook also Facebook Inc., USA – nur eine Hilfs- und Unterstützungsfunktion hat und in völliger Abhängigkeit von den Vorgaben der verantwortlichen Stelle agiert. Davon kann indes nicht die Rede sein, wenn – wie im vorliegenden Fall – die Tätigkeit der beauftragten Stelle über die Wahrnehmung von Hilfsfunktionen hinausgeht und diese die gesamte Verarbeitung weisungsunabhängig als eigene Angelegenheit ausführt.

Die amerikanische Gesellschaft Facebook Inc. tritt seit Erschaffung des Facebook-Netzwerkes 2004 als dessen Eigentümer und Betreiber auf. Sie bestimmt die Entwicklung des Facebook-Netzwerkes weltweit. Sie betreibt alle Rechenzentren, welche sich wiederum sämtlich in den USA befinden. Bis auf die Verarbeitung von Personendaten durch das User-Operations-Team in Dublin findet in Europa keinerlei Verarbeitung von Nutzerdaten

statt. Dass Facebook Inc., USA und Facebook Ireland Ltd. nicht zwei eigene, getrennte Dienste betreiben, zeigt schon die weltweit einheitliche optische und funktionale Gestaltung von Facebook. Eine Trennung der Verantwortlichkeiten erscheint im Rahmen des sozialen Netzwerks im Übrigen auch technisch ausgeschlossen. Die europäischen Nutzer sind in das Gesamtnetzwerk eingebunden. Ihre Daten können nicht getrennt und abgeschlossen von anderen Nutzergruppen gespeichert und verarbeitet werden, ohne die freie Kommunikation und Interaktion zwischen den verschiedenen Nutzern einzuschränken (insbesondere den Austausch und die Verlinkung des nutzergenerierten Contents). Handelt es sich nicht um eine Auftragsdatenverarbeitung, sondern ist Facebook Inc., USA – und nicht etwa Facebook Ireland Ltd. – als die verantwortliche Stelle anzusehen, hat dieses sowohl nach der europäischen Datenschutzrichtlinie als auch dem Bundesdatenschutzgesetz zur Folge, dass für die deutschen Nutzer des Dienstes nationales Datenschutzrecht anwendbar ist. Bei der Erhebung von Daten greift Facebook auf in Deutschland belegene Mittel zurück, indem es Cookies auf dem Rechner der Nutzer platziert. Mit der deutschsprachigen Facebook-Website wendet sich der Dienst darüber hinaus gezielt an Nutzer in Deutschland.

Selbst wenn man unterstellte, es läge eine Auftragsdatenverarbeitung von Facebook Inc., USA für Facebook Ireland Ltd. in Bezug auf deutsche und europäische Nutzer vor, so wäre gleichwohl Facebook Inc. für die Verarbeitung der Daten von beträchtlichen Teilen der deutschen und europäischen Nutzer verantwortlich. Denn Facebook Inc. ist bis Mai 2009 gegenüber sämtlichen Nutzern weltweit bei deren Registrierung als Vertragspartner aufgetreten. In dem hypothetischen Fall einer Auftragsdatenverarbeitung von Facebook Inc., USA für Facebook Ireland Ltd. hätte es also für bereits registrierte Nutzer zusätzlich einer wirksamen Überleitung der zivilrechtlichen Nutzungsverhältnisse bedurft, um die datenschutzrechtliche Verantwortlichkeit auf Facebook Ireland Ltd. zu übertragen. Zwar hat Facebook eine solche Überleitung mit der Änderung seiner Nutzungsbedingungen im Mai 2009 durch Austausch des Vertragspartners – Facebook Inc., USA durch Facebook Ireland Ltd. – versucht. Die Änderung der Nutzungsverhältnisse der bereits registrierten Nutzer ist jedoch unvereinbar mit deutschen und europäischen Klauselvorschriften und daher unwirksam. Folglich verfügen alleine in Deutschland mehrere Millionen Nutzer, die sich bis Mai 2009 registriert haben, nach wie vor über einen Vertrag mit Facebook Inc., USA. Insoweit ist Facebook Inc., USA in jedem Fall als die verantwortliche Stelle für die Verarbeitung von Daten im Rahmen des Facebook-Dienstes anzusehen (vgl. dazu ausführlich das o.g. Rechtsgutachten, S. 3 ff).

Die aufsichtsbehördliche Zuständigkeit für die Durchsetzung des eigenen Datenschutzrechtes gegenüber Facebook Inc., USA liegt nach der Europäischen Datenschutzrichtlinie bei dem jeweiligen Mitgliedsstaat. Für deutsche Nutzer liegt dementsprechend die Zuständigkeit für die Durchsetzung des Datenschutzrechts gegenüber Facebook Inc., USA bei den Aufsichtsbehörden der einzelnen Länder der Bundesrepublik Deutschland.

Selbst wenn man – entgegen der von uns vertretenen Auffassung – hypothetisch unterstellte, Facebook Ireland Ltd. sei für europäische Nutzer als verantwortliche Stelle anzusehen, so wäre nach dem oben Gesagten zwar irisches Datenschutzrecht für die gesamte EU anzuwenden; nach der europäischen Datenschutzrichtlinie wären die Aufsichtsbehörden der deutschen Bundesländer in Bezug auf die Facebook-Nutzer in Deutschland gleichwohl zuständig für die Durchsetzung des dann anwendbaren irischen Rechts gegenüber Facebook.

3.2 Freunde-Finder-Verfahren von Facebook

Freunde-Finder-Verfahren von Facebook musste wegen datenschutzrechtlicher Verstöße geändert werden.

Mitte Februar 2010 hat das weltweit größte soziale Netzwerk Facebook seine Vertriebsniederlassung für Deutschland in Hamburg bezogen. Seither haben uns viele Anschreiben von Bürgerinnen und Bürgern erreicht, die als Nichtnutzer von Facebook im Rahmen des Friend-Finding-Verfahrens Einladungen bekommen hatten. Sie waren darüber besorgt, dass Facebook Ihnen nicht nur Einladungen im Namen der Nutzer des Netzwerks, sondern zudem Bilder von weiteren Personen zusandte, die ihnen möglicherweise bekannt seien. Für die Angeschriebenen war es zutiefst beunruhigend, dass sie nicht wussten, wie es Facebook gelingen konnte, in Erfahrung zu bringen, dass sie die dort aufgeführten Personen in vielen Fällen kannten. Tatsächlich ist es durch das von Facebook praktizierte Verfahren des Friend-Finding möglich, weit reichende Beziehungsprofile anzulegen, die eben nicht nur auf Facebook-Nutzer bezogen sind, sondern auch auf Dritte, die mit dem Netzwerk nicht in Verbindung stehen. Wir haben daher das Freunde-Finder-Verfahren einer datenschutzrechtlichen Prüfung unterzogen.

Facebook erhält Daten von dritten Personen indem die Plattform die Nutzer dazu einlädt, persönliche Kontakte von ihrem E-Mail Provider oder aus ihrem Handy für Facebook zu öffnen. Unter der Funktion *„Freunde finden“ – „Finde Personen, denen Du E-Mails sendest“* bietet Facebook seinen Nutzern die Möglichkeit, ihre E-Mail-Adressbücher hochzuladen, um darin

potentielle Facebook-Kontakte ausfindig zu machen. Der Zugriff auf die Adressbücher erfolgt, indem der Nutzer die Zugangsdaten (E-Mail und Passwort) seines E-Mail-Kontos preisgibt, welches Facebook anschließend automatisch ausliest. Art und Umfang der im E-Mail-Adressbuch vorhandenen Kontaktdaten unterscheiden sich je nach E-Mail-Provider. Verarbeitet werden von Facebook stets die E-Mail-Adresse und in aller Regel der Name des Kontaktes. Facebook gleicht die so gewonnenen Kontaktdaten Dritter dann mit den Daten von Facebook-Mitgliedern ab, um danach entweder die Einladung eines Kontaktes in das Netzwerk (bei Nicht-Facebook-Nutzern) oder die Zusendung einer Freundschaftseinladung innerhalb des Netzwerkes (bei Facebook-Nutzern) vorzuschlagen.

Darüber hinaus bietet Facebook seinen Nutzern die Möglichkeit, die Adressbücher ihrer iPhones zu übermitteln, und zwar im Rahmen einer Synchronisierung mit dem Facebook-Account mittels der Facebook-App. Bei der Synchronisierung wird der gesamte Inhalt des iPhone-Adressbuches an Facebook gesandt (inkl. Telefonnummern und Email-Adressen). Umgekehrt werden bei diesem Vorgang auch die Kontaktdaten im iPhone mit bei Facebook bereits vorhandenen Nutzerdaten ergänzt, sofern der jeweilige Name übereinstimmt. Zum Versenden der Einladungen der hochgeladenen Kontakte wird dem Nutzer zunächst eine Liste derjenigen Kontakte präsentiert, die nicht Mitglied bei Facebook sind. Die vom Nutzer ausgewählten Kontakte erhalten dann eine E-Mail, mit der sie im Namen des Nutzers zum Beitritt in das Netzwerk eingeladen werden. In der bis Ende 2010 geltenden Version des Einladungsverfahren war der Inhalt der Einladungs-E-Mail von Facebook vorgegeben, lediglich die Sprache konnte eingestellt werden. Der Text wurde dem Nutzer weder vor noch nach dem Versenden der Einladung angezeigt. Facebook speicherte sodann die E-Mail-Adressen der bereits eingeladenen Personen, um später Erinnerungen versenden zu können. Sofern der Eingeladene sich nicht zwischenzeitlich registriert hatte, wurden noch Wochen später Erinnerungen im Namen des Nutzers versandt, ohne dass der Nutzer die E-Mail-Adresse dafür neu eingeben musste. Außerdem speicherte Facebook nicht nur die E-Mail-Adressen der Eingeladenen, sondern sämtliche aus dem E-Mail-Adressbuch des Nutzers hochgeladenen E-Mail-Adressen, solange der Nutzer oder die jeweilige Kontaktperson nicht ausdrücklich widersprachen. Facebook nutzte diese Daten, um seine Verbreitung und die Vernetzung unter den Mitgliedern zu fördern. Meldete sich zum Beispiel eine nicht eingeladene Kontaktperson später bei Facebook an, wurde ihr der Nutzer als Freund vorgeschlagen (ohne Zustimmung des Nutzers).

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat im Juli 2010 wegen der oben beschriebenen Vorgehensweise ein Buß-

geldverfahren gegen Facebook Inc. Palo Alto, USA wegen der Erhebung, Speicherung und Nutzung der Daten von Nichtnutzern zu Marketingzwecken ohne deren Einwilligung nach § 43 Abs. 2 Nr. 1 Bundesdatenschutzgesetz (BDSG) eingeleitet. Dem Verfahren liegt die folgende rechtliche Bewertung zugrunde:

Nach den derzeitigen Erkenntnissen wird das soziale Netzwerk ausschließlich von dem amerikanischen Anbieter betrieben. Die Verarbeitung der Daten findet in den USA statt. Bei der Niederlassung in Hamburg handelt es sich nur um ein Vertriebsbüro, das neue Werbepartner finden soll. Nach § 1 Abs. 5 S. 2 BDSG findet das Bundesdatenschutzgesetz auch dann Anwendung, wenn die für die Datenverarbeitung verantwortliche Stelle nicht in Deutschland, sondern in einem Staat außerhalb des EU/EWR-Raumes ansässig ist und wenn sie in Deutschland personenbezogene Daten erhebt, verarbeitet oder nutzt. Eine Erhebung von Daten findet in Deutschland statt, wenn die verantwortliche Stelle dabei auf in Deutschland belegene Mittel zurückgreift. Diese Voraussetzungen liegen vor (zu den Einzelheiten vgl. IV 3.1.). Es handelt sich nicht um eine ausschließlich persönliche oder familiäre Tätigkeit des Nutzers, die von der Beurteilung nach dem Bundesdatenschutzgesetz ausgenommen ist. Dies wäre nur dann der Fall, wenn zwischen dem Nutzer und dem Eingeladenen eine familiäre oder persönliche Beziehung bestünde, die versendeten Einladungen dem Nutzer als persönliche Nachrichten zurechenbar wären und Facebook die Kontakte lediglich zum Versenden der Einladungen nutzen würde. Bei dem beanstandeten Verfahren beim automatisierten Hochladen über das „Freunde finden“ bzw. die iPhone-Applikation gelangten Facebook jedoch unterschiedslos alle Kontakte zur Kenntnis, ohne dass der Nutzer eine Möglichkeit hatte, daraus nur die persönlich-familiären Kontakte auszuwählen. Auch wurden die von dem Nutzer nicht zur Einladung ausgewählten Kontakte durch Facebook nicht sofort gelöscht, sondern nur, wenn der Nutzer oder Nichtnutzer dies veranlasste. Schließlich nutzte das Netzwerk die auf diesem Weg gewonnenen Daten für eine unzulässige Direktwerbung in eigener Sache, in dem es dem Nutzer weder die Möglichkeit zur Einflussnahme auf den Inhalt der Nachricht (abgesehen von der Sprachauswahl) gab, noch ihm den Einladungstext überhaupt anzeigte. Hinzu kam, dass der Einladungstext mit einer Namensliste von Facebook-Nutzern angereichert wurde, die der Eingeladene zwar kennen konnte, die dem einladenden Nutzer jedoch grundsätzlich unbekannt waren. Für die Erinnerungsmails, deren Inhalt ebenfalls nicht vorab angezeigt wurde, galt das Gleiche. Bei dieser Sachlage konnte nicht von einer ausschließlich persönlichen Tätigkeit des Nutzers die Rede sein.

Die Erhebung von Daten von Nichtnutzern durch Facebook im Rahmen des Einladungsverfahrens und deren anschließende Speicherung war nach § 4 Abs. 1 in Verbindung mit § 28 Abs. 1 Nr. 2 BDSG unzulässig, da sie nicht zur Wahrung berechtigter Interessen von Facebook erforderlich war und einer solchen Speicherung überwiegende schutzwürdige Interesse der Betroffenen gegenüberstanden. Dies galt sowohl für die aus den E-Mail-Adressbüchern als auch für die aus den iPhone-Adressbüchern gewonnenen Daten. Das auf der Seite von Facebook grundsätzlich bestehende berechtigte Interesse an der Förderung des Wachstums des sozialen Netzwerkes war im Zeitpunkt des Versendens der Einladungen erreicht, eine darüber hinausgehende Speicherung der hochgeladenen Kontaktdaten war somit nicht erforderlich. Mit den schutzwürdigen Interessen der Betroffenen war es darüber hinaus nicht vereinbar, dass Facebook deren Daten zu dem Zweck speicherte, ihnen weitere „Erinnerungen“ senden zu können, nachdem sie auf eine erste Einladung nicht reagierten. Schließlich war zu beachten, dass das dargestellte Einladungsverfahren eine unzulässige Direktwerbung von Facebook an die Kontaktpersonen der Nutzer darstellte. Eine ohne Einwilligung per elektronische Post versandte Werbung verstößt jedoch gegen § 7 Abs. 2 Nr. 3 Gesetz gegen den unlauteren Wettbewerb (UWG) und ist daher unzulässig. Nach unseren Feststellungen erfolgte die unbefugte Datenerhebung und Speicherung der Daten Dritter durch Facebook auch in fahrlässiger Weise.

Nach Einleitung des Bußgeldverfahrens ist es uns in längeren Verhandlungen gelungen, mit Facebook eine Vereinbarung zu erzielen, die das Friend-Finding-Verfahren in vielen Punkten datenschutzkonform umgestaltet und zu erheblichen Verbesserungen für den Datenschutz geführt hat. Durch die Umgestaltung des Verfahrens sowohl beim Hochladen der E-Mail-Kontakte als auch bei der Synchronisierung der iPhone-Adressbücher, hat der Nutzer künftig eine transparente Kontrolle über die von ihm importierten Adressen. Vor allem wird er von Facebook auf seine besondere Verantwortung beim Importieren der Adressen und bei der Versendung der Einladungen hingewiesen. Die Nutzer erhalten zur eigenständigen Verwaltung der importieren Adressen ein Adressbuch, das den Nutzern die Speicherung und Löschung sowie die eigenständige Verwaltung der E-Mail-Kontakte für den Zweck der individuellen Einladung ermöglicht.

Zentraler Bestandteil der Vereinbarung ist der Schutz der Daten Dritter, also von Personen, die nicht Mitglied des Netzwerks sind, deren Daten gleichwohl durch den Nutzer auf Facebook importiert werden. Facebook verwendet diese E-Mail-Adressen nur noch für Zwecke der Freundsuche. Eine Verwendung zu anderen Zwecken ist ausgeschlossen.

Die Nutzung der E-Mail-Adressen Dritter zur Freundsuche ist danach nur noch in engen Grenzen zulässig: Der eingeladene Nicht-Facebook-Nutzer wird über einen Link in der Einladungs-E-Mail informiert, wie er in Zukunft verhindern kann, dass seine Adresse für Freundvorschläge verwendet wird. Hierzu wird dem Eingeladenen ein Opt-out zur Verfügung gestellt. Einladungen, die als Vorschlag Bilder von möglicherweise bekannten Personen umfassen, werden nur übersandt, wenn der Empfänger zuvor bereits eine Einladung (ohne Bilder) erhalten hat. Diese enthält den genannten Link und gibt dem Empfänger die Gelegenheit, einer Verwendung seiner E-Mail-Adresse für die Freundsuche zu widersprechen. Wer dem Einladungsverfahren widerspricht, kann so nicht nur verhindern, weitere Einladungen durch den Nutzer zu bekommen, – seine E-Mail-Adresse darf dann auch nicht zu Zwecken des Freunde-Findens durch Facebook verwendet werden. Die E-Mail-Adressen der Widersprechenden werden datenschutzkonform nur in Form eines Hash-Wertes, d.h. nicht im Klartext, gespeichert. Noch weitergehende Lösungen, etwa der gänzliche Verzicht auf das Importieren von Daten Dritter, waren in den Verhandlungen nicht zu erreichen. Sie dürften auch rechtlich kaum durchsetzbar sein.

Facebook hat das Verfahren – entsprechend der zugesagten Verbesserungen – Anfang des Jahres 2011 für deutsche Nutzer und später weltweit umgestaltet. Nach Veränderung des Verfahrens erreichten uns deutlich weniger Beschwerden und Anschreiben von eingeladenen Personen. Nach eingehender Abwägung hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit von einer Ahndung des bis zur Umgestaltung des Verfahrens unerlaubten Umgangs mit Daten aufgrund der seiner Zeit gezeigten Kooperationsbereitschaft von Facebook abgesehen.

3.3 Gesichtserkennung bei Facebook und Google

Die Biometrie-Datenbank von Facebook wird weiterhin als rechtswidrig angesehen. Aufgrund ergebnisloser Verhandlungen bereiten wir nun rechtliche Schritte vor.

Im Jahr 2011 haben die beiden sozialen Netzwerke Facebook und Google + (sprich „Google Plus“) die Funktion der Gesichtserkennung für ihre Mitglieder eingeführt.

Facebook hatte diese Technik in den USA schon einige Monate im Einsatz, bevor sie im Sommer 2011 für deutsche Nutzer freigeschaltet wurde. Google wartete – unter anderem aufgrund aufkommender Datenschutz-Kritik gegenüber Facebook – zunächst ab, nahm jedoch im Dezember 2011 ebenfalls die weltweite Einführung vor.

Seither wird bei jeder Veröffentlichung eines Fotos in den beiden Netzwerken automatisch versucht, darauf abgebildete Personen mittels eines biometrischen Erkennungsverfahrens zu identifizieren und – sofern es sich um Mitglieder des Netzwerks und „Freunde“ des jeweiligen Nutzers handelt – diese für eine namentliche Markierung auf dem Foto vorzuschlagen. Bestätigt der hochladende Nutzer den Namensvorschlag, wird das Bild mit dem Netzwerk-Profil der abgebildeten Person verknüpft, in der Sprache der Netzwerke: „getaggt“ (von engl. „Tag“ = „Markierung, Kennzeichen“).

Nach Aussage beider Netzwerke soll die Funktion die Nutzer entlasten und ihnen mehr Komfort und Bequemlichkeit beim Markieren von Bildern bieten. Aus unserer Sicht geschieht dies jedoch zu einem hohen Preis. Denn damit die Erkennung und Zuordnung von Gesichtern funktionieren kann, ist im Hintergrund eine gigantische Datenbank erforderlich, in der alle Mitglieder der Netzwerke detailliert mit ihren biometrischen Gesichtsmerkmalen erfasst und profiliert werden. Typische Merkmale zur Profilierung eines Gesichts sind beispielweise der Abstand von Augen, Ohren oder Mundwinkeln zueinander sowie deren jeweilige Entfernung zu markanten Gesichtspunkten wie Nasenspitze oder Kinn. Daraus werden für jedes Gesicht individuelle Kennzahlen errechnet, und im Gegensatz zur menschlichen Wahrnehmung, die sich durch Äußerlichkeiten wie Brille, Bart, Hautfarbe oder Schminke leicht irritieren oder täuschen lässt, ist die Erkennung durch Computer von unbeirrbarer Genauigkeit.

Eine biometrische Datensammlung ist daher höchst bedenklich, denn sie erlaubt die Identifizierung einer Person auch ohne ein Abbild als Vorlage – ein Datensatz mit beschreibenden Gesichtsparametern reicht aus. Diese Reduzierung menschlichen Aussehens auf mathematische Formeln birgt Brisanz: Während sich die Optik eines Menschen im Laufe seines Lebens durchaus ändert (meist aus Modegründen, aber auch durch Reife- und Alterungsprozesse), bleiben seine biometrischen Daten ab Erreichen des Erwachsenenalters weitgehend konstant. Biometrische Datensätze ermöglichen so die Identifizierung einer Person über Jahrzehnte und über den Tod hinaus.

Vor diesem Hintergrund wird die Schutzwürdigkeit des eigenen Gesichts von den meisten Menschen bislang verkannt. Dieses Merkmal ist kritischer als alle anderen persönlichen Daten wie Name, Adresse oder Telefonnummer, welche sich im Laufe des Lebens ändern oder bei Bedarf ändern lassen. Biometrische Daten jedoch sind jedem Menschen lebenslang zugeordnet, weil auf den Körper geschrieben.

Der großflächige Einsatz von Gesichtserkennung birgt daher unabsehbare Risiken für die Gesellschaft und hat das Potential, die Anonymität des Ein-

zelnen in der Öffentlichkeit und seine Grundrechte auf informationelle Selbstbestimmung binnen kurzer Zeit auszuhebeln. Täglich werden Millionen von Bildern und Videos auf die Server von Facebook und Google hochgeladen, in denen häufig auch Unbeteiligte erkennbar sind. Anhand dieser Gesichter könnten in Zukunft Aufenthalts- und Beziehungsprofile von Personen in bislang unvorstellbarem Umfang erstellt werden.

Da Facebook als „Pionier“ unter den beiden Netzwerken die automatische Gesichtserkennung quasi nebenbei, ohne ausreichende Nutzeraufklärung und vor allem ohne Einholung einer Zustimmung aktiviert hat, konnten wir die Einführung dieser Technologie nicht tatenlos hinnehmen. Die Gesichtserfassung war für alle Mitglieder standardmäßig freigeschaltet worden, obwohl europäische wie nationale Datenschutzgesetze hierfür eine unmissverständliche Einwilligungserklärung der Betroffenen fordern. Wir sind daher im August 2010 an Facebook herangetreten und haben im Wesentlichen folgende Forderungen formuliert:

- Einholung einer expliziten und informierten Zustimmung von den Nutzern zur Verarbeitung ihrer biometrischen Daten. Hierfür ist vor allem der Registrierungsprozess anzupassen. Der bislang praktizierte, pauschale Verweis auf die (mehrere Seiten umfassenden) Nutzungsbedingungen und Datenschutzrichtlinien ist für das sensible Thema Biometrie nicht ausreichend.
- Von den Millionen Deutschen, deren Gesichter bereits biometrisch erfasst wurden, muss die Zustimmung rückwirkend und eindeutig, d.h. mit Angabe von „Ja“ oder „Nein“, eingeholt werden. Bei „Nein“ ist das bislang erzeugte biometrische Profil des jeweiligen Nutzers zu löschen.
- Auch bei späterer Deaktivierung der Funktion durch den Nutzer sind alle über ihn gespeicherten biometrischen Informationen unverzüglich zu löschen
- Allgemein ist eine bessere und leichter auffindbare Aufklärung der Facebook-Mitglieder über diese Thematik nötig.

Die Verhandlungen mit Facebook haben sich über mehrere Monate und zahlreiche Gesprächstermine mit Unternehmensvertretern hingezogen. Die von Facebook vorgelegten schriftlichen Verbesserungsangebote blieben jedoch immer wieder hinter dem jeweils erreichten Verhandlungsstand zurück. So sahen wir im Dezember 2011 nur den Weg, ein Verwaltungsverfahren einzuleiten. Dessen Ziel ist die Verpflichtung des Unternehmens, die Vorgaben des deutschen und europäischen Datenschutzrechts umzusetzen. Zum Redaktionsschluss befand sich das Verfahren in der formellen Anhörung. Über das Ergebnis werden wir berichten.

Die medienwirksamen Diskussionen zu diesem Thema haben jedoch gefruchtet. Google hat bei der Einführung der Gesichtserkennung im eigenen Netzwerk „Google + “ unsere Forderungen im Vorhinein aufgegriffen. Die Entscheidung zur Teilnahme an der Gesichtserkennung obliegt dort komplett dem Nutzer, auf eine standardmäßige Voraktivierung wurde verzichtet. Auch das Thema Nutzeraufklärung wurde von Google deutlich datenschutzfreundlicher umgesetzt.

Dennoch müssen sich alle Mitglieder von Facebook und Google + bewusst sein, dass – auch wenn sie selbst nicht an der Gesichtserkennung teilnehmen – grundsätzlich jedes Bild, welches in die Netzwerke eingestellt wird, von „cleveren“ Algorithmen nach verwertbaren Gesichtern durchsucht wird. D.h. man liefert seine Freunde und sein soziales Umfeld der Gesichtserkennung aus. Nach den Aussagen beider Unternehmen sollen die Daten nicht zuordenbarer Gesichter (z. B. weil kein Mitglied im Netzwerk) zwar unverzüglich gelöscht werden. Diese Behauptung konnte von uns noch nicht überprüft werden, da der Nachweis ohne Zugriff auf die internen Systeme nicht geführt werden kann.

Anzumerken ist, dass Inhalt und Verlauf unserer Verhandlungen mit Facebook auch im Ausland auf großes Interesse stießen. So kamen Interview-Anfragen an den HmbBfDI nicht nur aus Europa, sondern auch aus den USA selbst. Dies führte zu Kontakten mit der dortigen nationalen Handelskommission FTC (Federal Trade Commission), die zur Vorbereitung eines Workshops über Gesichtserkennung auf unsere Erfahrungen zurückgreift.

3.4 Google Street View und die Folgen

Mit der Einhaltung der Zusagen durch Google ist die Problematik derartiger Dienste nicht erledigt. Vielmehr gilt es, das Augenmerk weiterhin darauf und auf neue Angebote zu richten.

Bereits im 22. Tätigkeitsbericht (IV 3.3.3) haben wir ausführlich über Google Street View berichtet. Zu diesem Zeitpunkt war der größte Teil der Fahrten der Google-Fahrzeuge bereits erfolgt, die Aufnahmen jedoch noch nicht veröffentlicht. Mittlerweile können die Bilder über Google-Maps und Google Earth aufgerufen werden.

Für uns war es wichtig, den Prozess der Einführung vor allen Dingen mit Blick auf die Einhaltung der Zusagen von Google Street View (veröffentlicht im 22.TB, IV 3.3.3) datenschutzrechtlich zu begleiten. Im Mittelpunkt unseres Interesses hat dabei gestanden, dafür Sorge zu tragen, dass die von

den Veröffentlichungen Betroffenen bereits vor der Veröffentlichung die Möglichkeit erhielten, die von Google abverlangten und schließlich auch eingeräumten Widerspruchsmöglichkeiten schon vor der Einstellung ins Internet effektiv wahrzunehmen.

Zunächst war es über einen Zeitraum von mehreren Monaten möglich, über das Internet, schriftlich, aber auch per Fax Widerspruch gegen die Abbildungen, die personenbezogene Daten enthielten, einzulegen. Google hatte ein Verfahren entwickelt, das es ermöglichte, bereits vor der Veröffentlichung eine Verpixelung von Hausansichten, Kfz und in Einzelfällen auch von Personen vorzunehmen. Von der Funktionsweise dieses Verfahrens überzeugten wir uns vor Ort. In Anbetracht der hohen Anzahl der Vorabwidersprüche kam es leider immer wieder zu Fällen, in denen sich die richtige Zuordnung als schwierig erwies. Dies führte dazu, dass sich etliche Betroffene mit Beschwerden an uns gewandt haben.

Im August 2010 hatten die Veröffentlichungspläne von Google konkretere Gestalt angenommen. Es wurde bekannt, dass zunächst die 20 größten Städte in Deutschland veröffentlicht werden sollen. Gleichzeitig hat das Unternehmen im Internet ein Tool zur Verfügung gestellt, das es Betroffenen ermöglicht hat, den Widerspruch direkt geltend zu machen. Für die 20 Städte der Erstveröffentlichung blieb das Tool einige Wochen geöffnet. Diesen Prozess haben wir intensiv begleitet und insbesondere auch eine Handreichung zu den Einzelheiten des konkreten Widerspruchsverfahrens veröffentlicht. Im November 2010 sind dann die Bilder der Straßenaufnahmen von 20 großen deutschen Städten durch Google im Internet veröffentlicht worden. Diese Veröffentlichung hat erneut zu einer erheblichen Anzahl von Beschwerden bei der Datenschutzaufsichtsbehörde geführt, etwa weil die Betroffenen mit der Umsetzung ihrer Widersprüche durch Google nicht zufrieden waren oder es umgekehrt seitens Google zu Verwechselungen gekommen war. Verwechselungen haben bedauerlicherweise auch dazu geführt, dass in wenigen Fällen die Aufnahmen von Grundstücken Betroffener verpixelt worden waren, die gar keinen Widerspruch eingelegt hatten. Es ist jedoch anzumerken, dass sich diese Schwierigkeiten auf Einzelfälle beschränkten und sich das Vorabwiderspruchsverfahren – auch wenn es einen großen Aufwand erforderte – bewährt hat.

Im Frühjahr 2011 hat das Unternehmen entschieden, neben den bereits erfolgten Veröffentlichungen keine Aufnahmen weiterer deutscher Orte mehr zu veröffentlichen.

Widersprüche gegen die bereits im Internet verfügbaren Bilder sind relativ problemlos in der Weise einzulegen, dass auf den Internet-Abbildungen

von Google Street View links unten die Anwendung „Ein Problem melden“ aufgerufen werden kann. Wenn etwas zu beanstanden ist, kann diese Anwendung durch Anklicken geöffnet werden. Es erscheint eine Seite, auf der einzelne Probleme angeklickt werden können: Bedenken in Bezug auf die Privatsphäre, Unangemessener Inhalt oder Sonstiges, jeweils mit eigenen Unterpunkten. Anschließend sollte das Problem in dem dafür vorgesehenen Feld beschrieben werden. Die Angabe einer E-Mailadresse ist erforderlich. In der Bildvorschau ist der Problempunkt einzugrenzen.

Die Anzahl der Beschwerden über die Unkenntlichmachungen in den veröffentlichten Bildern hat in den letzten Monaten 2011 deutlich abgenommen, was darauf hindeutet, dass die jetzt praktizierte Widerspruchsmöglichkeit von den Betroffenen angenommen wird und im Ergebnis deren Wünsche im Hinblick auf eine datenschutzrechtlich einwandfreie Gestaltung des Dienstes Rechnung trägt.

Schon zu Beginn der Beschäftigung der Datenschutzaufsichtsbehörden mit dieser Thematik ist deutlich geworden, dass die Generalklauseln des Bundesdatenschutzgesetzes für die Erhebung von Geodaten wenig taugliche Regulierungsgrundlagen sind (vgl. schon 21. TB IV 3.3). Vor diesem Hintergrund hat Hamburg im Frühjahr 2010 einen Antrag zur Änderung des Bundesdatenschutzgesetzes in den Bundesrat (Drucksache 259/10) eingebracht, der wenig später durch einen Änderungsantrag von Rheinland-Pfalz ergänzt wurde. Bedauerlicherweise wurde diese Bundesratsinitiative von der Bundesregierung abgelehnt. Stattdessen hat jedoch im September 2010 beim Bundesminister des Innern ein Spitzengespräch stattgefunden, an dem Vertreter der Datenschutzbeauftragten, Wirtschaft, Politik und Verwaltung teilnahmen. Ziel des Gesprächs sollte die gemeinsame Entwicklung von Lösungsmöglichkeiten sein. Ergebnis dieser Zusammenkunft war die Erwartung an die Wirtschaft, bis Dezember 2010 einen sogenannten Datenschutzkodex zu Google Street View und vergleichbaren Diensten vorzulegen. Gleichzeitig ist eine Gesetzesinitiative angekündigt worden, die den Schutz vor besonders schweren Persönlichkeitsverletzungen im Internet verbessern soll („Rote-Linie-Gesetz“). Dazu sind Eckpunkte veröffentlicht worden.

Anfang Dezember 2010 hat dann der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) einen Datenschutzkodex für Geodatendienste vorgestellt. Angesichts erheblicher Kritik an diesem Datenschutzkodex seitens der Datenschutzaufsichtsbehörden fand im Februar 2011 in Düsseldorf ein Gespräch zwischen dem Düsseldorfer Kreis und Vertretern der BITKOM statt, an dem auch eine Vertreterin unserer Dienststelle teilnahm. Im Ergebnis hat sich die BITKOM nicht auf die Vorstellungen der Vertreter des Düsseldorfer Kreises hinsicht-

lich der datenschutzgerechten Gestaltung eines entsprechenden Kodex eingelassen, so dass es zu keiner Übereinstimmung über den Inhalt des Kodex kam. Gleichwohl beruft sich die Internetwirtschaft derzeit auf die Grundlagen, die dieser Kodex vorgibt.

Im April 2011 wurde ein Beschluss des Düsseldorfer Kreises zum Datenschutz-Kodex des BITKOM für Geodatendienste erlassen, die Unzulänglichkeiten des Kodex darstellt. Dieser Beschlusss ist abrufbar unter: *https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2011/Datenschutz-Kodex_unzureichend/Datenschutzkodex_unzureichend.pdf.* Darin wird bemängelt, dass das Widerspruchsrecht – anders als von uns bei Google durchgesetzt – erst nach der Veröffentlichung der Bilder vorgesehen ist. Darüber hinaus werden viele Beeinträchtigungen der Privatsphäre von dem Kodex nicht erfasst, ebenso besteht keinerlei Bindung aller Unternehmen in Deutschland, sondern es handelt sich um eine freiwillige Unterwerfung derjenigen Unternehmen, die den Kodex unterzeichnen.

Mittlerweile hat auch Microsoft begonnen, Aufnahmen für den Dienst Bing Maps Streetside zu fertigen. Gegen die Veröffentlichung von Gebäuden erhielten die Betroffenen die Möglichkeit, auch in diesem Fall im Vorwege Widerspruch einzulegen. Insgesamt hat dieses Verfahren, obwohl ähnlich, zumindest in Hamburg deutlich weniger öffentliche Aufmerksamkeit auf sich gezogen, als es in den Jahren vorher bei Google Street View zu verzeichnen war. Zuständige Datenschutzaufsichtsbehörde für Microsoft ist das bayerische Landesamt für Datenschutzaufsicht in Ansbach.

Insgesamt zeigt der Umgang mit diesen Verfahren, dass es nicht ausreicht, es der Wirtschaft zu überlassen, einen eigenen Kodex zu erarbeiten, der noch dazu von den Datenschutzaufsichtsbehörden als nicht dem Bundesdatenschutzgesetz entsprechend bewertet wurde. Notwendig sind verlässliche gesetzliche Vorschriften, die für alle Anbieter gleichermaßen verbindlich sind.

3.5 Erfassung von Funknetzen durch Google im Rahmen von Street View

Die Erfassung von WLAN-Netzen durch Google führte zu einem globalen Datenschutzdesaster. Die Abarbeitung der dabei entstandenen Probleme beschäftigt uns noch immer.

Im April 2010 haben wir erfahren, dass die Firma Google im Zuge der Befahrungen für den Dienst Street View (siehe IV 3.4 und 22. TB, IV 3.3) Funknetze privater Betreiber systematisch erfasst hat. Gegenstand dieser Erfassung sind die WLAN-Netze gewesen, die jeweils in Reichweite der

Street-View-Fahrzeuge zu empfangen waren. Ziel dieser Aktion war es, eine Datenbasis für Lokalisierungsdienste zu schaffen bzw. diese zu ergänzen.

Trotz ausführlicher, bis in das Jahr 2009 zurückgehender Gespräche mit uns hat Google weder uns noch eine andere Aufsichtsbehörde über diese Datenerhebung informiert. Wir haben die Tatsache der WLAN-Erfassung in einer gemeinsamen Presseerklärung mit dem Bundesdatenschutzbeauftragten am 22. April 2010 kritisiert und einen sofortigen Stopp der Erhebung gefordert. Google hat hierauf mit dem Verweis darauf reagiert, dass es sich bei den erfassten WLAN-Daten um öffentlich und für jedermann empfangbare Signale handele und kein Personenbezug bestehe.

Wir haben daraufhin den Vorstand der Google Inc. um schriftliche Aufklärung ersucht und eine Prüfung der WLAN-Erfassungs- und Aufzeichnungstechnik angekündigt. Dabei sollte u. a. festgestellt werden, welche Daten der einzelnen WLAN erhoben und verarbeitet werden und wie diese Informationen in die Lokalisierungsdienste bei Google integriert werden.

Kurze Zeit später musste Google seine bisherigen Äußerungen revidieren und gab am 14. Mai 2010 per Unternehmensblog bekannt, dass auch Kommunikationsinhalte (sog. Payload) solcher WLAN-Netze aufgezeichnet worden sind, die unverschlüsselt betrieben wurden. Diese Aufzeichnung sei irrtümlich erfolgt und für den gewünschten Zweck nicht erforderlich. Als Sofortmaßnahme wurde die weitere Erfassung von WLAN-Netzen durch Street-View-Fahrzeuge ausgesetzt.

Zum Hintergrund: Für den Betreiber einer Mobilfunkplattform, etwa Google mit seinem Smartphone-Betriebssystem Android, ist eine möglichst genaue Erfassung der Standorte von WLAN-Netzen von großer Bedeutung. Für einen Nutzer, der mit einem Smartphone unterwegs ist, besteht häufig die Anforderung, seinen Standort zu bestimmen, z. B. um eine Wegbeschreibung zu erhalten oder ein Restaurant in der Nähe zu finden. Zwar steht hierfür das satellitenbasierte GPS-System zur Verfügung, doch dieses hat eine Reihe von Nachteilen. So dauert die Ortung per GPS mitunter recht lange und steht in Gebäuden oder unter Bäumen nicht oder nur eingeschränkt zur Verfügung.

Als Alternative hat sich daher die Orientierung anhand der empfangbaren WLAN-Netze etabliert. Dabei wird der von einem Smartphone aktuell empfangbare WLAN-Bestand mit der vorab erstellten Datenbank eines Dienstleisters abgeglichen und daraus der Standort ermittelt. Je genauer und aktueller die Datenbank ist, desto präziser funktioniert die Ortung. Sie ist auch möglich, wenn nicht alle WLAN, die die Datenbank enthält, eingeschaltet sind oder empfangen werden können. Zumindest in dicht besie-

delten Gegenden sind ausreichend WLAN in Betrieb, um das Verfahren zuverlässig zu betreiben. Aktualisierungen der Datenbank werden zudem aus den Anfragen der Smartphones selbst erzeugt, da diese den aktuellen WLAN-Bestand mitliefern.

Welche Daten der WLAN für ein solches Verfahren erforderlich sind, ist eine Frage, die im Rahmen der datenschutzrechtlichen Bewertung zu klären ist. Dass die übertragenen Kommunikationsinhalte jedenfalls nicht dazu gehören, ist offensichtlich.

Aufgrund des Eingeständnisses seitens Google, dass auch Inhaltsdaten aufgezeichnet und dauerhaft gespeichert wurden, erfolgte eine weltweite Befassung verschiedener Datenschutz- und Strafverfolgungsbehörden, u. a. in Frankreich, Spanien, Holland, den USA und Kanada. Auch in Deutschland ist aufgrund verschiedener Anzeigen die Staatsanwaltschaft Hamburg tätig geworden. Deren Verfahren ist noch nicht abgeschlossen. Ein eventuelles Einschreiten durch unsere Behörde ist daher aktuell gehemmt. Wir müssen den Ausgang des staatsanwaltschaftlichen Verfahrens abwarten.

Allerdings haben wir unterdessen die Sachverhaltsaufklärung in verschiedener Hinsicht vorangetrieben. Zum einen waren wir in die Ermittlungen der Staatsanwaltschaft eingebunden, die wir bei ihrer Analyse der genauen Aufzeichnungspraxis der Street-View-Fahrzeuge unterstützen konnten. Zum anderen haben wir eine Analyse der von Google aufgezeichneten Daten vorgenommen, um das Ausmaß der Datenschutzverstöße abschätzen zu können.

Die WLAN-Erfassung durch Google hat zu Diskussionen über die Frage des Personenbezugs der Daten geführt, die in diesem Zusammenhang erhoben wurden. Hierzu gehören:

- Die SSID, d.h. der vom Betreiber frei wählbare Name des Netzwerks.
- Die MAC-Adresse, d.h. die vom Hersteller des WLAN-Routers fest vorgegebene Hardwareadresse.
- Der Funkkanal.
- Die Signalstärke an einem bestimmten Ort.
- Der Verschlüsselungsstatus.

Auf europäischer Ebene ist hieraus eine Position der Artikel-29-Gruppe entstanden („Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten“, abrufbar unter *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_de.pdf).* Diese kommt zu der „Schlussfolgerung, dass die Kombination einer MAC-Adresse und einem

WI-Fi-Zugangspunkt mit seinem berechneten Standort als personenbezogene Daten zu behandeln ist."

Aus dieser Position wird die Forderung abgeleitet, dass der Betreiber eines WLAN gegen die Erfassung seiner Daten widersprechen können muss. Seitens Google wurde diese Forderung im November 2011 in der Form aufgegriffen, dass solche WLAN, deren SSID auf „_nomap" endet, künftig nicht mehr in die Lokalisierungsdatenbank aufgenommen werden. Der Betreiber eines WLAN, der diesem bisher z. B. den Namen „hmbbfdi1" gegeben hat, könnte es daher in „hmbbfdi1_nomap" umbenennen, um Google zu signalisieren, dass er keine Verwendung für Lokalisierungszwecke wünscht.

In diesem Zusammenhang sind einige technische Fragen aufgetaucht, die die genauen Verarbeitungsprozesse betreffen. Google hat sich dahingehend geäußert, dass „_nomap"-WLAN zwar aus der Lokalisierungsdatenbank entfernt werden, jedoch zugleich in eine Art Widerspruchsdatenbank eingetragen werden. Wie dies genau erfolgt und ob es erforderlich und zulässig ist, ist Gegenstand unserer weiteren Klärungen.

3.6 Selbstregulierung bei Sozialen Netzwerken

Jede Selbstregulierung durch die Wirtschaft kann nur dann Bestand haben, wenn sie den gesetzlichen Vorgaben entspricht.

Schon seit geraumer Zeit raten Datenschützer dazu, im Umgang mit Sozialen Netzwerken vorsichtig zu sein und besonders die Privatsphäreeinstellungen sorgfältig vorzunehmen (vgl. zuletzt 22. TB, IV 3.2). In den letzten Jahren hat jedoch nicht nur das Angebot an in- und ausländischen Betreibern von Sozialen Netzwerken zugenommen, auch die Nutzung breitet sich rasant über alle Bevölkerungs- und Altersstrukturen hinweg aus.

Uns erreichen immer wieder Beschwerden Betroffener, die sich durch Soziale Netzwerke aus dem In- und Ausland in ihren Persönlichkeits- und Datenschutzrechten beeinträchtigt fühlen. Darüber hinaus nehmen wir im Rahmen unserer Kapazitäten Kontrollen vor, die jedoch durch das Fehlen spezifischer gesetzlicher Grundlagen erheblich erschwert werden (vgl. IV 3.2, 3.3). Dabei ist es in der Vergangenheit mit den Anbietern der Sozialen Netzwerke immer wieder zu Diskussionen über die Anwendbarkeit und die Auslegung der geltenden datenschutzrechtlichen Bestimmungen gekommen. Unseres Erachtens besteht kein Zweifel an der Anwendbarkeit deutschen Datenschutzrechts (vgl. hierzu IV 3.1). Dennoch ist es zur Klarstellung und Präzisierung dringend erforderlich, auf nationaler, europäischer und internationaler Ebene spezielle Vorschriften zu schaffen, die sich mit diesen Themen möglichst umfassend auseinandersetzen.

Das Bundesministerium des Innern hat im November 2011 Anbieter Sozialer Netzwerke, Verbände, Verbraucher- und Datenschützer zu einem Gespräch über eine „Selbstregulierung im Internet“ eingeladen. Dabei hat es auch auf den Datenschutzkodex der BITKOM zu den Geodaten Bezug genommen, der für klare Regeln und Transparenz gesorgt habe. Gerade dieser Datenschutzkodex sorgt aber bei den Datenschutzaufsichtsbehörden für ausgesprochene Skepsis gegenüber den Selbstverpflichtungen der Wirtschaft. Der Datenschutzkodex zu den Geodaten aus dem Jahre 2010 (vgl. im Einzelnen IV 3.4) enthält etliche datenschutzrechtliche Unzulänglichkeiten und sollte nicht als Beispiel für eine funktionierende Selbstregulierung der Wirtschaft herangezogen werden.

Gleichwohl können Selbstverpflichtungen gesetzliche Regelungen durchaus im positiven Sinne ergänzen und auf diese Weise den Datenschutz der Betroffenen verbessern, wenn sie mit wirksamen Sanktionsmechanismen verbunden werden. Eine rechtliche Verbindlichkeit ist aber nur zu erreichen, wenn sie der zuständigen Datenschutzaufsichtsbehörde nach § 38a BDSG zur Prüfung vorgelegt wird.

Damit die Selbstverpflichtung nicht hinter den gesetzlichen Anforderungen zurückbleibt, hat der Düsseldorfer Kreis in seiner Sitzung vom November 2011 einen Beschluss erlassen, der auch die inhaltlichen Anforderungen an eine derartige Selbstverpflichtung präzisiert und abgerufen werden kann unter: *https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2011/Datenschutz_in_sozialen_Netzwerken/Datenschutz_in_sozialen_Netzwerken_endgueltig.pdf*.

Dem Inhalt einer möglichen Selbstregulierung im Internet durch die Wirtschaft sehen wir mit großem Interesse entgegen.

3.7 Minderjährigenschutz in Sozialen Netzwerken

Der Schutz Minderjähriger vor den Folgen der Nutzung Sozialer Netzwerke sollte auch ein Anliegen der Anbieter solcher Plattformen sein.

Es ist zu beobachten, dass Kinder und Jugendliche das Internet nicht nur nutzen, um sich über sie interessierende Themen zu informieren. Vielmehr nehmen sie verstärkt auch an Sozialen Netzwerken wie Facebook, SchülerVZ und speziell auf sie zugeschnittene Angeboten teil. Dies birgt die Gefahr, dass gerade jüngere Nutzer durch die Anbieter – aber auch durch andere Nutzer – verleitet werden, personenbezogene Daten über sich und ihre Familie einschließlich sensibler Daten, die nicht für die Öffentlichkeit bestimmt sind, preiszugeben.

Neben der Aufklärung von Kindern und Jugendlichen durch Eltern, Lehrer und Medien sind auch die Anbieter derartiger Netzwerke gefordert, Lösungen zu entwickeln, die die datenschutzrechtlich risikoarme Teilnahme an den Angeboten ermöglichen.

Der Düsseldorfer Kreis hat sich mit dieser Thematik sehr intensiv auseinandergesetzt und in seiner Sitzung im November 2010 einen Beschluss gefasst, der abrufbar ist unter: *https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2010/Minderjaehrige_in_sozialen_Netzwerken/Minderjaehrige_in_sozialen_Netzwerken_wirksamer_schuetzen.pdf.*

3.8 Anonyme Bezahlverfahren im Internet

Sofern Internet-Anbieter künftig ihre Angebote verstärkt nur noch gegen Bezahlung zur Verfügung stellen, muss darauf geachtet werden, dass die Bezahlung auch anonym oder pseudonym ermöglicht wird.

Insbesondere Webseitenbetreiber, die Informationsdienste oder Medieninhalte über das Internet zur Verfügung stellen, haben ihr Angebot bereits kostenpflichtig gemacht oder planen dies für die Zukunft. § 13 Abs. 6 des Telemediengesetzes bestimmt, dass der Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen hat, soweit dies technisch möglich und zumutbar ist. Darüber ist der Nutzer zu informieren. Diese Vorschrift soll gewährleisten, dass sich jeder – ohne sich identifizieren zu müssen oder als Nutzer bestimmter Angebote nachvollziehbar zu werden – frei aus diesen Quellen informieren kann. Wirklich umgesetzt werden kann dies jedoch erst dann, wenn Bezahlverfahren angeboten werden, die anonym, zumindest aber pseudonym ausgestaltet sind. Die Verlagerung der Bezahlung auf dritte Unternehmen, die dann wieder eine Identifizierung der Betroffenen vornehmen müssen, reicht hierfür nicht aus.

In diesem Zusammenhang ist es wichtig zu erwähnen, dass die Internetwirtschaft dabei auf die Unterstützung der Kreditwirtschaft angewiesen ist. Seitens der Kreditwirtschaft wurde es in der Vergangenheit versäumt, für diese Zwecke datenschutzgerechte Verfahren anzubieten oder zu unterstützen. Vorstellbar ist die Entwicklung sogenannter „Whitecards“, die anonym aufgeladen werden können.

Besorgniserregend ist jedoch, dass ein aktueller Gesetzesentwurf der Bundesregierung zum Geldwäschegesetz (BT-Drs. 17/6804) möglicherweise dazu führt, dass eine solche Entwicklung unterbunden wird. Dies hat bereits die 82. Konferenz der Datenschutzbeauftragten des Bundes und

der Länder in einem Beschluss bemängelt, der unter *http://www.sachsen-anhalt.de/index.php?id = 51849* abrufbar ist.

Der Düsseldorfer Kreis hat sich den darin enthaltenen Forderungen angeschlossen und im November 2011 einen Beschluss zur Ermöglichung anonymen und pseudonymen elektronischen Bezahlens von Internet-Angeboten erlassen: *https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2011/Anonymes_und_pseudonymes_elektronisches_Bezahlen_von_Internet-Angeboten/17_elektronisches_Bezahlen.pdf.*

4. Reichweitenmessung

4.1 Google Analytics

Bei dem Produkt Google Analytics konnten erhebliche datenschutzrechtliche Verbesserungen erreicht werden. Weitere Anpassungen sind dennoch erforderlich.

Bereits im 22. Tätigkeitsbericht haben wir über Google Analytics und andere Trackingsysteme berichtet (22. TB, IV 3.4). Hinweisen möchten wir noch einmal besonders auf den dort abgedruckten Beschluss des Düsseldorfer Kreises vom November 2009, an dem die Trackingsysteme in der privaten Wirtschaft gemessen werden. Dieser Beschluss ist auch unter *http://www.datenschutz-mv.de/dschutz/beschlue/Analyse.pdf* veröffentlicht.

Nachdem wir Google über den Beschluss des Düsseldorfer Kreises informiert hatten, haben wir zunächst auch verschiedene Webseitenanbieter angeschrieben und auf die Unzulässigkeit des Einsatzes dieses Reichweitenmessungs-Systems hingewiesen. Angesichts der Verarbeitung von personenbezogenen Daten im Zusammenhang mit der Nutzung einzelner Webseiten liegt die rechtliche Verantwortung für den datenschutzgerechten Einsatz nicht direkt bei dem Produktanbieter – in diesem Fall Google –, sondern bei den Anbietern der jeweiligen Seiten.

Damit ist jede Datenschutzaufsichtsbehörde rechtlich befugt, bei den Webseitenanbietern in ihrem Zuständigkeitsbereich Kontrollen vorzunehmen. Allerdings wurde im Rahmen des Düsseldorfer Kreises der Datenschutzaufsichtsbehörden vereinbart, dass wir federführend die Verhandlungen mit Google mit dem Ziel eines im Hinblick auf den Datenschutz verbesserten Produkts führen. Diese Tatsache war dem Umstand geschuldet, dass die einzelnen Webseitenanbieter das Produkt nicht verändern können und damit nur vor der Wahl standen, es entweder unverändert einzusetzen oder ganz davon Abstand zu nehmen. Durch eine Pressemitteilung im Februar 2010 wurden die Webseitenbetreiber durch uns deutlich auf ihre

Verantwortung aufmerksam gemacht. Die Verhandlungen mit Google haben wir in engem Zusammenwirken mit den übrigen Datenschutzaufsichtsbehörden geführt. Ziel war es, alle in dem Beschluss des Düsseldorfer Kreises aufgeführten Voraussetzungen für den datenschutzgerechten Betrieb eines solchen Analyseverfahrens umzusetzen.

Bereits im Februar 2010 hat Google erste Vorschläge zur Verbesserung von Google Analytics vorgelegt. Diese waren jedoch in keiner Weise geeignet, unsere Bedenken auszuräumen. Allerdings war schon zu diesem – aus heutiger Sicht frühen Zeitpunkt – zu erkennen, dass das Unternehmen bereit war, eine Kürzung der IP-Adresse vorzunehmen und auch die eigentlich von den Webseitenbetreibern auf der Grundlage des Telemediengesetzes umzusetzende Widerspruchsmöglichkeit in den Dienst zu implementieren.

Ende des Jahre 2010 waren die Verhandlungen so weit gediehen, dass Google ein sogenanntes Widerspruchs-Plugin entwickelt hatte, das es den Nutzern von Webseiten, auf denen Google Analytics installiert ist, ermöglichen soll, Widerspruch gegen die Nutzung ihrer Daten zu Analysezwecken einzulegen. Neben weiteren Änderungsvorschlägen wurde uns zu diesem Zeitpunkt auch der Entwurf eines Vertrages zur Auftragsdatenverarbeitung übersandt. Der Abschluss eines solchen Vertrages zwischen den Webseitenbetreibern und Google ist rechtlich erforderlich, weil es sich u. a. bei den erhobenen IP-Adressen – die dann bei Google gekürzt werden – um personenbezogene Daten handelt. Da der Betreiber der Webseite, wie bereits erwähnt, für die Erhebung der Daten bei der Nutzung seines Dienstes selbst und nicht Google verantwortlich ist, muss er auch dafür sorgen, dass er nach den Vorschriften des Bundesdatenschutzgesetzes die Fäden der Datenverarbeitung in der Hand behält. Zu diesem Zweck schließ er mit Google einen Vertrag zur Auftragsdatenverarbeitung, die den Umfang der Datenverarbeitung durch Google und die Kontrollrechte der Webseitenbetreiber rechtlich verbindlich beschreibt. Nur so kann ein mit dem Datenschutzrecht im Einklang stehender Einsatz gewährleistet werden.

Vor diesem Hintergrund könnte man meinen, dass jeder einzelne Webseitenbetreiber einen eigenen Vertrag zur Auftragsdatenverarbeitung entwickeln und mit Google abschließen müsste. Angesichts der Notwendigkeit für Google, die Geschäftsprozesse mit einer Vielzahl von Nutzern des Produkts Google Analytics zu standardisieren, legte Google den Datenschutzaufsichtsbehörden einen Vertragsentwurf zu Kommentierung vor. Nach Vorlage des ersten Entwurfs hat es noch einige Monate gedauert, bis die zunächst vorhandenen Schwächen des Vertrages durch Verhandlungen mit Google ausgeräumt werden konnten. Google hat zugesagt,

99,99999% der IP-Adressenkürzungen in Europa vorzunehmen. Eine abgestimmte Fassung des Vertrages ist Voraussetzung für den rechtskonformen Einsatz des Dienstes. Webseitenbetreiber, die Analytics nutzen wollen, dürfen den Vertragsabschluss daher nicht als bloße Formalie ansehen. Vielmehr sollte ihnen der Vertrag noch einmal deutlich machen, dass sie es sind, die für die personenbezogenen Daten ihrer Nutzer datenschutzrechtlich die Verantwortung tragen.

Erst im September 2011 konnten wir mittels einer Pressemitteilung öffentlich bekannt geben, dass die Nutzung des Dienstes Google Analytics unter Beachtung der beschriebenen Vorgaben nunmehr durch uns nicht mehr beanstandet wird. Der vollständige Wortlaut ist im Internet abrufbar unter http://www.datenschutz-hamburg.de/news/detail/article/beanstandungsfreier-betrieb-von-google-analytics-ab-sofort-moeglich.html.

Zusammengefasst sind für uns neben anderen notwendigen Anpassungen des Produkts drei Aspekte von entscheidender Bedeutung:

- Den Nutzern wird die Möglichkeit zum Widerspruch gegen die Erfassung von Nutzungsdaten eingeräumt. Google stellt ein so genanntes Deaktivierungs-Add-On zur Verfügung (http://tools.google.com/dlpage/gaoptout?hl=de). Dieses Add-On war bisher für Internet Explorer, Firefox und Google Chrome verfügbar. Google hat nun Safari und Opera hinzugefügt, so dass alle gängigen Browser berücksichtigt werden.
- Auf Anforderung des Webseitenbetreibers wird das letzte Oktett der IP-Adresse vor jeglicher Speicherung gelöscht, so dass darüber keine Identifizierung des Nutzers über die IP-Adresse mehr möglich ist. Der Prozess der Kürzung der Adresse erfolgt innerhalb Europas.
- Zwischen den Webseitenbetreibern und Google wird ein Vertrag zur Auftragsdatenverarbeitung nach den Vorschriften des Bundesdatenschutzgesetzes abgeschlossen.

Angesichts der Tatsache, dass die Webseitenbetreiber an den Verhandlungen nicht unmittelbar beteiligt waren und verständlicherweise Fragen zur Umsetzung der datenschutzrechtlichen Vorgaben beim Einsatz von Google Analytics aufgetreten sind, haben wir die „Hinweise für Webseitenbetreiber mit Sitz in Hamburg, die Google Analytics einsetzen“ veröffentlicht unter: *http://www.datenschutz-hamburg.de/uploads/media/Google-Analytics_Hinweise_Webseitenbetreiber_in_Hamburg.pdf*

Dennoch kann unter diese Thematik noch kein Schlusspunkt gesetzt werden. Vielmehr bleiben trotz der positiven Ergebnisse der Verhandlungen mit Google noch einige Punkte klärungsbedürftig. Noch gibt es beispiels-

weise keine Lösung für eine Übertragung der Widerspruchsmöglichkeit auf mobilen Endgeräten, z. B. Smartphones, die in der Regel andere als die genannten Browser einsetzen. Wir haben Google aufgefordert, zu diesem Punkt Stellung zu nehmen und Lösungsmöglichkeiten vorzuschlagen. Google hat zugesagt, Lösungen zu entwickeln. Die zunehmende Nutzung mobiler Endgeräte wird die Problematik deutlich verschärfen. Außerdem bleibt abzuwarten, welche Auswirkungen die Umsetzung der E-Privacy-Richtlinie und die Einführung des neuen technischen Standards bei der Adressenvergabe im Internet (IPv6) haben werden.

4.2 hamburg.de

Die Prüfung der Reichweitenmessung bei hamburg.de hatte weitreichende Folgen.

Auch hamburg.de wurde von uns auf die Vereinbarkeit der eingesetzten Reichweitenmessungen mit den datenschutzrechtlichen Vorschriften und dem Beschluss des Düsseldorfer Kreises vom November 2009 überprüft (vgl. hierzu auch die Ausführungen unter IV 4.1). Dabei stellte sich heraus, dass das über hamburg.de vermittelte Angebot keineswegs den datenschutzrechtlichen Vorgaben entsprach. Insbesondere wurde die vollständige IP-Adresse des Nutzers zur Reichweitenmessung erfasst und verwendet. Darüber hinaus wurden permanente und Session-Cookies gesetzt, ohne dass dem Nutzer eine handhabbare Widerspruchsmöglichkeit zur Verfügung stand. Auch ein Vertrag zur Datenverarbeitung im Auftrag war nicht gesetzeskonform.

Zunächst gestalteten sich die Gespräche vor allem deswegen als schwierig, weil auch die einzelnen Behörden der Stadt – zu Beginn der Prüfung sogar wir selbst – verantwortliche Stellen im Sinne des Datenschutzrechts waren. Wir stellten bereits zu Beginn klar, dass die verantwortlichen Stellen der Stadt ihre Verantwortung für die Erhebung, Verarbeitung und Nutzung wahrnehmen müssen und schalteten zudem unsere eigene Internetpräsenz bei hamburg.de ab, um unserer Verantwortung gerecht zu werden, nachdem die Speicherung von IP-Adressen durch die verantwortlichen Stellen eingeräumt wurde. Die datenschutzgerechte Umstellung wurde jedoch erschwert durch die Tatsache, dass allein hamburg.de den technischen Rahmen für die Gestaltung der einzelnen Angebote zur Verfügung stellt und die Verantwortlichen von hamburg.de immer wieder darauf verwiesen, an der Gestaltung des problematischen Analysetools SZM (Skalierbares Zentrales Messsystem) nichts ändern zu können. Sie seien auf eine vertragliche Zusammenarbeit mit der Firma INFOnline angewiesen,

die als technischer Dienstleister für die IVW (Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V.) die Online-Reichweite des Stadtportals hamburg.de messen würden. Diese vertraglichen Beziehungen seien grundlegende Voraussetzung für die Vermarktung von Werbeplätzen und folgten direkt aus der Mitgliedschaft in der IVW, die als Verein der Werbewirtschaft und Publizierenden in Deutschland diesbezüglich eine einzigartige Rolle innehabe. Ein Austritt aus diesen Vertragsbeziehungen komme daher nicht infrage, weil damit schwerwiegende wirtschaftliche Folgen verbunden wären. Darüber hinaus könne es zu nachteiligen Wirkungen für den Medienstandort Hamburg kommen.

Die von dem Unternehmen vorgetragenen Argumente hatten keinerlei Auswirkungen auf die datenschutzrechtliche Bewertung unsererseits, zeigen aber die weit über hamburgische Unternehmen hinausgehende Relevanz dieser Angelegenheit. Daher haben wir – ganz ähnlich wie bei Google Analytics – Kontakt zu dem Anbieter des Analysetools SZM, INFOnline, aufgenommen. Gleichzeitig haben wir auch die übrigen Datenschutzaufsichtsbehörden über diese Gespräche informiert, weil die Angelegenheit auch auf deutschlandweit sämtliche Webseitenanbieter, die SZM einsetzen, Auswirkungen hat. Erst diese Verhandlungen, an denen neben Vertretern der Stadt und von hamburg.de auch INFOnline und IVW teilnahmen, brachten den Durchbruch.

INFOnline stellte das Verfahren in der Weise um, dass die von den Nutzern erfassten IP-Adressen vor jeder weiteren Verarbeitung um das letzte Oktett gekürzt werden, um den Personenbezug zu entfernen. Darüber hinaus wurde das Verfahren um die gesetzlich vorgeschriebene Widerspruchsmöglichkeit erweitert. Unter http://optout.ivwbox.de kann der Widerspruch jetzt einfach eingelegt werden. Die vertragliche Beziehung zwischen den jeweiligen Seitenbetreibern als Auftraggeber und INFOnline wurde den Anforderungen des Bundesdatenschutzgesetzes entsprechend angepasst. Die Anpassung des Vertrages ist in enger Abstimmung zwischen INFOnline und uns erfolgt.

Diese Vorgehensweise über den Anbieter des Verfahrens hatte den entscheidenden Vorteil, dass davon nicht nur eine verantwortliche Stelle, sondern deutschlandweit alle Anbieter profitieren, die das SZM-Verfahren einsetzen. Immerhin handelt es sich dabei um 1300 Webseitenbetreiber.

In Hamburg werden wir in Kürze einige dieser Anbieter daraufhin überprüfen, ob z. B. die Verträge zur Auftragsdatenverarbeitung in der vorgesehenen Weise abgeschlossen wurden.

5. Versicherungswirtschaft

5.1 Einwilligungs- und Schweigepflichtentbindungserklärung

Nach langjährigen Erörterungen wurde zwischen den Datenschutzaufsichtsbehörden und der Versicherungswirtschaft ein Mustertext für eine Einwilligungs- und Schweigepflichtentbindungserklärung abgestimmt.

Im Berichtszeitraum konnte nach langjährigen Verhandlungen (vgl. zuletzt 22. TB, IV 4.1) zwischen Datenschutzaufsichtsbehörden und Versicherungswirtschaft eine weitestgehende Einigung über den Mustertext für eine Einwilligungs- und Schweigepflichtentbindungserklärung erzielt werden. Die Klausel betrifft den Umgang der Versicherungen mit Gesundheitsdaten und sonstigen nach § 203 des Strafgesetzbuchs geschützten Daten. Sie ist notwendig, da die Vorschriften des Bundesdatenschutzgesetzes und des Versicherungsvertragsgesetzes keine ausreichenende Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten durch Versicherungen enthalten. Die mehrseitige Mustererklärung bildet den maximalen Rahmen für eine Einwilligungs- und Schweigepflicht-Entbindungserklärung ab. Werden darin Datenverarbeitungen beschrieben, die von dem jeweiligen Unternehmen nicht durchgeführt werden, sollen die entsprechenden Absätze des Mustertextes nicht verwendet werden.

Durch die Klausel sollen nur die tatsächlich einwilligungsbedürftigen Datenverarbeitungsprozesse geregelt werden. Datenverarbeitungen, die auf eine gesetzliche Grundlage gestützt werden können und keiner Einwilligung bedürfen, werden davon nicht erfasst. Diese sollen in den Verhaltensregeln der Versicherungswirtschaft konkretisiert werden (siehe dazu unten). Die Versicherungsunternehmen sind aufgefordert, die bisherigen Einwilligungstexte zeitnah durch neue zu ersetzen, die der Mustererklärung entsprechen.

5.2 Verhaltensregeln

Die Erörterung der Verhaltensregeln hat zu einer Annäherung zwischen den Datenschutzaufsichtsbehörden und der Versicherungswirtschaft geführt, die Verhandlungen dauern indes noch an.

Nach Abstimmung der Einwilligungs- und Schweigepflichtentbindungserklärung sind die Gespräche über den von der Versicherungswirtschaft vorgelegten Entwurf für Verhaltensregeln wieder aufgenommen worden. Im 22. Tätigkeitsbericht (IV 4.2) hatten wir darüber berichtet, dass die Mehrheit der Datenschutzaufsichtsbehörden den bis zu diesem Zeitpunkt vorliegenden Entwurf für Verhaltensregeln nach § 38 a Bundesdaten-

schutzgesetz noch nicht für datenschutzkonform hielt. Der Entwurf ist zwischenzeitlich mehrfach überarbeitet worden. Die zuvor umstrittenen Regelungen zu Bonitätsabfragen und zum Scoring wurden in den Verhaltensregeln durch sog. Platzhalteregelungen ersetzt. Danach sollen in diesen Bereichen zunächst die gesetzlichen Regelungen weiter gelten, bis sich Aufsichtsbehörden und Versicherungswirtschaft auf eine abgestimmte Regelung verständigt haben. Auch bezüglich der Verwendung der Daten für Zwecke der Werbung verweisen die Verhaltensregeln nunmehr auf die gesetzlichen Regelungen des Bundesdatenschutzgesetzes.

Die Versicherungswirtschaft möchte die Verhaltensregeln möglichst zeitgleich mit der neuen Einwilligungs- und Schweigepflichtentbindungserklärung einführen, damit Betriebsabläufe und IT-Prozesse nur einmal angepasst werden müssen. Nur so könnten die Versicherungsunternehmen auch Rechtssicherheit für alle vormals die Datenschutzeinwilligungserklärung regelnden Fragen (vgl. 20. TB, 20.1.) erhalten. Wir werden über den Fortgang berichten.

5.3 Warn- und Hinweissystem

Das neue Hinweis- und Informationssystem (HIS) der Versicherungswirtschaft wird seit dem 1. April 2011 als Auskunftei betrieben.

Nach jahrelangen Verhandlungen zwischen den Datenschutzaufsichtsbehörden und der Versicherungswirtschaft (vgl. zuletzt 22. TB, IV 4.3) ist das Hinweis- und Informationssystem der Versicherungswirtschaft umstrukturiert worden. Seit dem 1. April 2011 wird es durch die Informa Insurance Risk and Fraud Prevention GmbH in Baden-Baden betrieben. Über das HIS werden keine Gesundheitsdaten ausgetauscht. Zuständige Datenschutzaufsichtsbehörde für das Unternehmen ist der baden-württembergische Datenschutzbeauftragte. Einzelne datenschutzrechtliche Fragestellungen im Zusammenhang mit der Nutzung des HIS werden auch weiterhin in der Arbeitsgruppe Versicherungswirtschaft erörtert werden.

6. Auskunfteien

6.1 Auskunft gegen Ausweiskopie

Unter bestimmten Umständen ist es zulässig, dass Auskunfteien Betroffene, die ihr Auskunftsrecht nach § 34 BDSG geltend machen, zur Übersendung einer Ausweiskopie auffordern.

Auskunfteien sind nach § 34 Abs. 1 Bundesdatenschutzgesetz (BDSG) verpflichtet, den Betroffenen Auskunft über die über sie gespeicherten Daten einschließlich Herkunft und Empfänger der Daten zu erteilen. Um sicherzustellen, dass die Auskünfte nur die Betroffenen, keinesfalls aber unbe-

rechtigte Dritte erreichen, verlangen Auskunfteien in der Regel mit dem Antrag auf Auskunft die Vorlage einer Kopie des Personalausweises.

Über diese Praxis haben sich viele Betroffene – in der Regel telefonisch – bei der Datenschutzaufsichtsbehörde beschwert. Sie befürchteten, mit der Übersendung der Personalausweisdaten den Auskunfteien mehr Daten zur Verfügung zu stellen, als diese bereits über sie haben. Derartige Beschwerden erreichten auch die Aufsichtsbehörden anderer Bundesländer. Angesichts der besonderen Problematik, die mit der Weitergabe von Personalausweiskopien verbunden sein kann, hat sich die bundesweite Arbeitsgruppe Auskunfteien des Düsseldorfer Kreises intensiv mit diesem Thema befasst.

Einerseits ist zu bedenken, dass die Auskunft nach § 34 Abs. 1 BDSG jedem Betroffenen nach dem Gesetzeswortlaut ohne weitere Bedingungen zu erteilen ist. Der Gesetzgeber selbst hat die Auskunftserteilung nicht von der Vorlage einer Legitimation abhängig gemacht. Darüber hinaus enthält die vollständige Kopie eines Personalausweises in der Tat Angaben, die in der Regel bei Auskunfteien nicht zur Verfügung stehen und dort auch nichts zu suchen haben, wie etwa die Größe der Betroffenen oder deren Augenfarbe. Daher ist es nicht ohne weiteres einsichtig, dass Auskunfteien sich weigern, den Betroffenen ohne die Einreichung einer Ausweiskopie die Auskunft zu erteilen.

Andererseits legen auch die Datenschutzaufsichtsbehörden besonderen Wert darauf, dass Auskünfte tatsächlich die Betroffenen selbst und nicht unberechtigte Dritte erreichen. Darin könnte sogar eine Ordnungswidrigkeit wegen fahrlässiger unbefugter Übermittlung personenbezogener Daten zu sehen sein, die mit einem erheblichen Bußgeld (bis zu 300000 €) geahndet werden kann. Dies führt dazu, dass eine telefonische Auskunftserteilung in der Regel für unzulässig erachtet wird, obwohl § 34 BDSG die Form der Auskunftserteilung selbst nicht festlegt. Zu bedenken ist in diesem Zusammenhang, dass die in einer Auskunft enthaltenen Daten teilweise sensibel sind und Dritte durch ihre Neugier oder ihr Interesse durchaus verleitet sein können, sich ohne das gesetzlich geforderte berechtigte Interesse derartige Daten zu verschaffen. Die Aufforderung zur Vorlage der Ausweiskopie kann insoweit als eine gewisse Hürde angesehen werden, den Auskunfteien eine zusätzliche Gewähr für die Identität der Betroffenen zu bieten, die Unberechtigte nur unter dem Einsatz zusätzlicher krimineller Energie überwinden können.

Nach Diskussion der unterschiedlichen Argumente mit Vertretern der Auskunfteien in der Arbeitsgruppe des Düsseldorfer Kreises konnte Einver-

nehmen darüber erzielt werden, dass in folgenden Fällen künftig grundsätzlich auf die Vorlage von Ausweiskopien verzichtet werden kann:

– Betroffene machen ihren Auskunftsanspruch nach § 34 BDSG in einem zeitlichen Zusammenhang zu einer vorherigen Benachrichtigung nach § 33 BDSG geltend (bis zu vier Wochen nach der Benachrichtigung).
– Die Auskunftei hat keine Bonitäts- oder sonstigen Inhaltsdaten (Negativ- oder Positivdaten) zu der betroffenen Person gespeichert.

In der ersten Fallgruppe besteht angesichts des zeitlichen Zusammenhangs zu der Benachrichtigung die Vermutung, dass Betroffene sich zusätzlich noch über den Inhalt der Auskunft und auch über den Empfänger informieren wollen und erst durch die Benachrichtigung den Anstoß zur Geltendmachung ihres Auskunftsanspruchs erhalten haben. Die Wahrscheinlichkeit, dass ausgerechnet in diesem zeitlichen Zusammenhang ein Dritter in Missbrauchsabsicht die Auskunft anfordert, ist gering. Die zweite Fallgruppe ist dadurch gerechtfertigt, dass keine weiteren relevanten Daten bezüglich der Betroffenen mitgeteilt werden.

Die Datenschutzaufsichtsbehörden haben gegenüber den Auskunfteien deutlich gemacht, dass die Betroffenen darauf hingewiesen werden müssen, dass in den Ausweiskopien alle über die erforderlichen Daten hinausgehenden Angaben geschwärzt werden können. Insbesondere sollten durch die Betroffenen die Seriennummer und die sechsstellige Kartenzugangsnummer geschwärzt werden, damit diese Nummern nicht zum Auslesen der Daten aus dem kontaktlosen Chip oder zum Freischalten der PIN missbraucht werden können. Erforderlich für die Identifizierung durch Auskunfteien sind Name, Anschrift, Geburtsdatum und Gültigkeitsdauer des Ausweises. Die Angabe des Geburtsortes kann verlangt werden, wenn auch bei der Auskunftei ein entsprechendes Datum vorliegt. Die Ausweiskopie darf ausschließlich zu Identifizierungszwecken verwendet werden und ist danach umgehend zu vernichten. Eine automatisierte Speicherung der Ausweisdaten ist nach § 20 Abs. 2 PAuswG unzulässig.

Aus unserer Sicht werden mit einer solchen Verfahrensweise einerseits keine unüberwindbaren Hindernisse für die Betroffenen aufgestellt, andererseits wird aber auch sichergestellt, dass die Auskunfteien ihrer Pflicht zur Identifizierung der Betroffenen in angemessener Weise nachkommen können.

6.2 Fehlerhafte Auskunftserteilung

Mehrere fehlerhafte Auskunftserteilungen durch eine Wirtschaftsauskunftei wurden mit einem Bußgeld geahndet.

Durch mehrere Beschwerden ist uns bekannt geworden, dass eine Wirtschaftsauskunftei Betroffenen unrichtige Auskünfte erteilt hat. Obwohl das Unternehmen durchaus regelmäßig Auskünfte erteilt und auch bemüht ist, in diesem Punkt die datenschutzrechtlichen Anforderungen einzuhalten, führte die Organisation des Unternehmens, das in verschiedene verantwortliche Stellen aufgeteilt war, zu nicht nur unrichtigen Auskünften, sondern darüber hinaus auch zu unrechtmäßigen unternehmensübergreifenden Erhebungen personenbezogener Daten der Betroffenen. Diese Verfahrensweise wurde unsererseits mit einem Bußgeld geahndet.

Mittlerweile haben Änderungen in dem Unternehmen und der Auskunftspraxis dazu geführt, dass die Auskunftserteilung den datenschutzrechtlichen Anforderungen entspricht.

7. Kreditwirtschaft

7.1 Unbefugte Weitergabe von Kundendaten

Ohne Einwilligung der Kunden dürfen Bankdaten weder zu Beratungs- noch zu Marketingzwecken an Dritte weitergegeben werden.

Medienberichten im Juli 2010 war zu entnehmen, dass die Hamburger Sparkasse Personen, die als externe Finanzberater tätig sind, seit Jahren im Rahmen des sog. „mobilen Vertriebs“ den Zugriff auf Daten ihrer Kunden gestattet hat. Wegen des Verdachts der unbefugten Weitergabe von personenbezogenen Kundendaten an Dritte haben wir die Angelegenheit unverzüglich überprüft und dabei Folgendes festgestellt:

Die Hamburger Sparkasse AG hat im Zeitraum von 2007 bis 2010 in einer unbestimmten Anzahl von Fällen den für sie arbeitenden mobilen Vertriebsmitarbeitern einen Zugriff auf Kundendaten erlaubt, ohne dass für die Weitergabe eine Rechtsgrundlage existierte. Insbesondere lag keine Einwilligungserklärung der Kunden vor.

Seit Ende 2005 arbeitete die Hamburger Sparkasse mit mobilen Vertriebsmitarbeitern zusammen. Dabei handelte es sich um Finanzberater, die auf Provisionsbasis als selbständige Gewerbetreibende nach § 84 HGB nach Angabe der Hamburger Sparkasse nur für diese Bank Finanzprodukte verkauften. Laut Aufgabenbeschreibung in einer Stellenanzeige sollten die selbständigen Finanzberater neue Kundenpotenziale der Hamburger Sparkasse ausschöpfen, neue Kundenbeziehungen durch eine aktive Kundenansprache erschließen und Bank- und Finanzprodukte, insbesondere Vorsorgeprodukte der Hamburger Sparkasse verkaufen. Die selbständigen Finanzberater führten die Geschäfte von den Filialen aus. Im Jahr 2010

arbeiteten ca. 80 freie Finanzberater für die Haspa, von denen jeder 4-5 Filialen betreut hat.

Die mobilen Vertriebsmitarbeiter hatten bis zum 9. Juli 2010 Zugriff auf den gesamten Kundendatenbestand der Hamburger Sparkasse mit Kundenstammdaten und sämtlichen Kundenkonten. Zu den Kundendaten gehörte auch die Bezeichnung des Kundentyps. Ein großer Teil der Kunden wurde seit 2007 unter Nutzung des Marketing-Instruments „Sensus“ in bestimmte Typen eingeteilt: Bewahrer, Performer, Abenteurer, Hedonisten, Disziplinierte, Tolerante und Genießer. Dabei wurden die Kundenstammdaten und die von den Kunden genutzten Produkte zur Erstellung der Profile ausgewertet. Die Typisierung sollte den Finanzberatern eine auf die individuellen Bedürfnisse ausgerichtete Ansprache der Kunden ermöglichen.

Grund für die unbeschränkte Zugriffsmöglichkeit der mobilen Vertriebsmitarbeiter auf die gesamten Kundendaten war nach Angaben der Hamburger Sparkasse die von allen Sparkassen eingesetzte Software, deren Funktionsumfang eine technische Beschränkung der Zugriffe nicht ermöglichte. Da technische Zugriffsbeschränkungen auf der Kundendatenbank nicht möglich waren, hatte die Hamburger Sparkasse organisatorische Regeln für die Zugriffe bzw. Zugriffsbeschränkungen aufgestellt, die in einer Dienstanweisung enthalten waren. Diese enthielt unter anderem die Regelung, dass den Handelsvertretern die Einsicht in Daten von Kunden nicht gestattet war, die keine entsprechende Einwilligungserklärung unterschrieben hatten und dass die vom Kunden unterschriebene Einwilligungserklärung Voraussetzung für die Provisionszahlung war. Die Einwilligungserklärungen wurden von Bankmitarbeitern eingeholt, zentral in die Datenbank eingepflegt und dort aufbewahrt.

Anhand der in Logprotokollen erfassten Zugriffe auf die Kundendatenbank wurde durch die Revisionsabteilung regelmäßig stichprobenhaft geprüft, welche Finanzberater auf welche Daten zugegriffen haben. Auf Nachfrage der Datenschutzaufsichtsbehörde teilte die Hamburger Sparkasse das Ergebnis der Stichprobenauswertungen der Jahre 2007 bis 2010 mit.

Daraus ergab sich, dass im Jahr 2007 in 38 Fällen, 2008 in 35 Fällen, 2009 in 9 Fällen und 2010 in 585 Fällen durch mobile Vertriebsmitarbeiter auf Kundendaten zugegriffen wurde, obwohl für die Abfragen keine schriftlichen Einwilligungserklärungen der Kunden vorlagen. Da es sich nur um Stichproben handelte, ist davon auszugehen, dass die tatsächliche Anzahl der unbefugten Zugriffe noch weitaus höher gelegen hat.

Wir haben daraufhin nach § 43 Abs. 2 Nr. 1 und Nr. 2 in Verbindung mit Abs. 3 BDSG ein Bußgeld in Höhe von 200.000 Euro verhängt, da die Hamburger Sparkasse unbefugt personenbezogene Daten, die nicht allgemein zu-

gänglich waren, durch die Möglichkeit des Abrufs an Dritte übermittelt hatte (§ 3 Abs. 4 Nr. 3b BDSG). Der Weitergabe der Kundendaten an die mobilen Vertriebsmitarbeiter, die als selbständige Handelsvertreter Dritte im Sinne des § 3 Abs. 8 Satz 2 BDSG waren, standen die überwiegenden schutzwürdigen Interessen der Kunden, die keine Einwilligungserklärung abgegeben hatten, sowie das Bankgeheimnis entgegen. Die den mobilen Vertriebsmitarbeitern eingeräumte Abrufberechtigung war von Anfang an zu weitgehend, da die organisatorische Regelung eine Zugriffskontrolle nicht gewährleistete und das technische Zugriffsrecht vom Vorliegen einer Einwilligung unabhängig war.

Bei der Verhängung des Bußgeldes sind wir davon ausgegangen, dass in mehr als 600 Fällen durch mobile Vertriebsmitarbeiter unbefugte Zugriffe auf Kundendaten erfolgt sind, da keine schriftlichen Einwilligungen vorlagen. Hinzu kam, dass auch in den Fällen, in denen Kunden schriftliche Einwilligungen erteilt hatten, diese sich nicht auf die Weitergabe der Daten zur Erstellung des Kundenprofils bezogen. Denn die Kunden wurden über die Klassifizierung weder schriftlich noch mündlich informiert und konnten daher in die Weitergabe dieser Daten nicht wirksam einwilligen. Die Anzahl der ohne wirksame Einwilligung vorgenommen Zugriffe durch die mobilen Vertriebsmitarbeiter war daher um ein Vielfaches höher als die Stichproben nahelegten. Angebliche mündliche Einwilligungen der Kunden, auf die das Kreditinstitut hingewiesen hatte, wurden nicht als Rechtsgrundlage akzeptiert, da mündliche Einwilligungen nach dem Bundesdatenschutzgesetz nur unter ganz besonderen Umständen – z. B. bei Eilbedürftigkeit und einer unzumutbaren Beeinträchtigung durch die Schriftform – zulässig sind. Derartige Umstände lagen jedoch nicht vor.

Das Kreditinstitut hat sich bei der Aufklärung des Datenschutzverstoßes kooperativ verhalten, die erforderlichen Auskünfte erteilt und Einsicht in die Datenbank gewährt. Unverzüglich nach Bekanntwerden des Vorwurfs hat die Hamburger Sparkasse den mobilen Vertriebsmitarbeitern die Berechtigung des Zugriffs auf die Kundendatenbank entzogen. Seitdem wird ein geändertes technisches Verfahren eingesetzt, das den Anforderungen des Datenschutzes gerecht wird, da vor der Einräumung des Zugriffs technisch im Einzelfall überprüft wird, ob eine Einwilligungserklärung der Kunden vorliegt.

Die durch den Einsatz der Methode des Neuromarketing gewonnenen „Sensus-Kundendaten“ wurden aus der Kundendatenbank gelöscht. Unseren Bedenken gegen diese Form der Nutzung von Kundendaten, die die schutzwürdigen Interessen der Kunden außer Acht lässt und gegen den Datenschutz verstößt, wurde somit Rechnung getragen. Wir haben mit dem Unternehmen vereinbart, dass die „Sensus-Kundendaten“ für eine

vorübergehende Zeit auf Mikrofilmen aufbewahrt werden dürfen, um Auskunftsersuchen der Kunden beantworten zu können. Der Zugriff auf die Mikrofilme ist wenigen Personen vorbehalten. Spätestens nach 2 Jahren müssen auch diese Daten gelöscht werden.

8. Handel

8.1 Datenverarbeitung beim EC-Lastschriftverfahren

Händler und Abwickler von EC-Lastschriftverfahren dürfen Transaktionsdaten nur zur Abwicklung der Zahlung und im engen Rahmen zur Missbrauchsbekämpfung einsetzen.

In unserem 11. Tätigkeitsbericht aus dem Jahr 1992 (27.2) hatten wir die Datenverarbeitung zur Abwicklung des EC-Lastschriftverfahrens des Handels und die rechtlichen Rahmenbedingungen für eine datenschutzrechtlich zulässige Ausgestaltung des Verfahrens dargestellt. Das damals mit dem Handel abgesprochene Verfahren ist durch Ausdehnung des Systems auf immer größere Teile des Einzelhandels sowie die Einschaltung von Dienstleistern zur Durchführung und Abwicklung des Verfahrens verändert und erheblich ausgeweitet worden, ohne dass die datenschutzrechtlichen Anforderungen dabei berücksichtigt worden sind.

Aufgrund von Beschwerden und Presseberichten haben sich die Datenschutzaufsichtsbehörden in den Jahren 2010 und 2011 intensiv mit den Datenverarbeitungsprozessen bei der Durchführung des EC-Lastschriftverfahrens beschäftigt. Die Bezahlung im EC-Lastschriftverfahren ist im Handel weit verbreitet, weil es nicht so teuer wie das EC-Cash-Verfahren ist, bei dessen Einsatz der Händler von der Bank des Kunden eine Zahlungszusage erhält. Demgegenüber trägt beim Lastschriftverfahren der Händler das Risiko, dass eine Lastschrift des Kunden nicht eingelöst werden kann.

Die meisten Einzelhändler wickeln das EC-Lastschriftverfahren nicht selbst ab, sondern beauftragen Dienstleister, die so genannten EC-Netzbetreiber. Diese stellen in der Regel die Kartenlesegeräte zur Verfügung und wickeln die Zahlungen ab. Bei der Bezahlung im EC-Lastschriftverfahren werden aus der EC-Karte der Kunden Bankleitzahl, Kontonummer, Kartenverfallsdatum und die so genannte Kartenfolgenummer ausgelesen und zusammen mit den Daten der Transaktion wie Höhe der Forderung, Zeitpunkt und Ort der Handlung erfasst. Sodann werden diese Daten mit bei dem Netzbetreiber gespeicherten Datenbeständen über frühere Transaktionen eines Kunden abgeglichen. Während dieser Abgleich sich zunächst auf eine Prüfung beschränkte, ob ein Kunde bei dem jeweiligen Händler in der Vergangenheit eine Lastschrift nicht bezahlt hatte, haben die Netzbetreiber ihre Leistungen in den letzten Jahren erheblich erweitert. Neben

dem Abgleich mit der Sperrdatei der Rücklastschriften eines Händlers wurden händlerübergreifende Sperrdateien gebildet und die Transaktionsdaten auch damit abgeglichen.

Außerdem geben Netzbetreiber aufgrund der bei ihnen zu den Transaktionen eines Kunden gespeicherten Daten häufig auch Zahlungswegeempfehlungen ab. Dabei werden nicht nur negative Rücklastschriften ausgewertet, sondern alle Lastschrift-Zahlungen eines Kunden innerhalb eines bestimmten Zeitraums, die über den Netzbetreiber abgewickelt wurden. Diese Auswertung kann dazu führen, dass dem Kunden an der Kasse nur das EC-Cash-Verfahren angeboten wird, weil er ein vom Händler gesetztes Limit (Lastschriftzahlungen nur bis zu einem bestimmten Betrag innerhalb eines Monats) überschritten hat. Darüber hinaus speichern und nutzen die Netzbetreiber zum Teil händlerübergreifend Transaktionsdaten aus Zahlungsvorgängen im EC-Lastschriftverfahren, um bestimmte Muster zu erkennen, die auf eine missbräuchliche Kartennutzung und damit auf einen Forderungsausfall hindeuten können.

Die von den Kunden beim Einkauf zu unterzeichnenden Klauseln auf den Lastschriftbelegen sind in den vergangenen Jahren immer länger, unübersichtlicher und unverständlicher geworden. Eine wirksame Einwilligung in die oben dargestellte Datenverarbeitung können die Kunden durch ihre Unterschrift nicht erteilen, da die Texte häufig kaum lesbar sind und nur unzureichend oder gar nicht über die Datenverarbeitungsvorgänge informieren. Hinzu kommt, dass eine wirksame Einwilligung nach § 4a BDSG vor der Datenverarbeitung erfolgen müsste, die Unterschrift des Kunden jedoch erst nachträglich nach der automatisierten Erfassung der Transaktionsdaten abgegeben wird.

Die Datenschutzaufsichtsbehörden haben Netzbetreiber und Händler aufgrund datenschutzrechtlicher Bedenken zu einer Änderung des Verfahrens aufgefordert. Da nach mehrheitlicher Auffassung die Erteilung einer wirksamen Einwilligung durch die Kunden in die Verarbeitung der Transaktionsdaten aufgrund der besonderen Situation beim Bezahlen an einer Kasse (insbesondere Eile, Druck durch andere wartende Kunden) kaum möglich ist, wurde eine Beschränkung auf Datenverarbeitungsprozesse gefordert, die nach § 28 Abs. 1 Satz 1 Nr. 1 und 2 BDSG gerechtfertigt sind. Eine Einwilligung der Kunden in die Datenverarbeitung ist dann nicht mehr erforderlich.

Es wurde daher in einer gemeinsamen Arbeitsgruppe, an der auch wir beteiligt waren, mit den Wirtschaftsvertretern eine Änderung der Datenverarbeitung des Lastschriftverfahrens vereinbart, die von der Mehrheit der Aufsichtsbehörden akzeptiert wird. Netzbetreiber und Händler dürfen

Transaktionsdaten nach § 28 Abs. 1 Nr. 1 und 2 BDSG künftig nur noch zwecks Prüfung und Durchführung einer Zahlung sowie für wenige Tage zur Verhinderung von Kartenmissbrauch verarbeiten. Zu diesem Zweck dürfen Rücklastschriftinformationen von allen bei einem Netzbetreiber angeschlossenen Händlern genutzt werden. Hierüber müssen die Kunden durch einen deutlich sichtbaren Aushang an den Kassen unterrichtet werden. Falls Zahlungsinformationen wegen der Festlegung von Händlerlimits ausgewertet werden sollen, sind die Kunden auch darüber in dem Aushangtext zu unterrichten. Die Nutzung für andere Zwecke und eine über wenige Tage hinausgehende Speicherung der Transaktionsdaten ist nicht erlaubt.

Netzbetreiber und Vertreter des Handels haben angekündigt, schnellstmöglich das Verfahren zu ändern und durch deutlich sichtbare Aushänge vor den Kassen die Kunden künftig vor der Bezahlung darüber zu unterrichten, zu welchen Zwecken ihre Daten im Lastschriftverfahren verarbeitet werden. Auch die Texte auf den Lastschriftbelegen werden geändert.

8.2 Weitergabe von Transaktionsdaten durch Netzbetreiber an Tochtergesellschaft

Eine Nutzung von Transaktionsdaten, die im EC-Lastschriftverfahren anfallen, für eigene Zwecke des Netzbetreibers ist unzulässig.

Im Oktober 2010 haben wir die Kopie einer Präsentation der Firma Easycash Loyalty Solutions GmbH für ein Geschäftsmodell erhalten, in der das Unternehmen für die Erstellung von Zahlungsverkehrsanalysen durch die Verknüpfung von Transaktionsdaten für den bargeldlosen Zahlungsverkehr und personenbezogenen Daten von Kundenkarten geworben hat. Das Unternehmen ist ein führender Anbieter im Bereich von Kunden- und Gutscheinkarten in Europa und eine Tochtergesellschaft der Easycash GmbH mit Sitz in Ratingen, Nordrhein-Westfalen. Die Easycash GmbH wickelt im Auftrag von verschiedenen Einzelhandelsunternehmen das elektronische Lastschriftverfahren für EC-Kartenkunden ab, welche die Kunden an dem Bezahlterminal der Händler mittels EC-Karte auslösen. Bei den dabei erfassten Transaktionsdaten handelt es sich neben der EC-Nummer und der Bankleitzahl der Kunden im Wesentlichen um Daten zu den gekauften Waren, dem Kaufpreis, dem Datum und der Uhrzeit.

Wegen des Verdachts einer unzulässigen Datenverarbeitung haben wir eine unangemeldete Vor-Ort-Prüfung durchgeführt. Dabei haben sich zunächst keine konkreten Anhaltspunkte für einen Abgleich zwischen Transaktionsdaten, die im EC-Lastschriftverfahren anfallen, und den von der Easycash Loayalty Solutions GmbH verarbeiteten Kundenkartendaten

in dem befürchteten großen Ausmaß ergeben. Nach Angaben der Easycash Loyalty Solutions GmbH habe man zwar ein Modell zur Erstellung von Zahlungsverkehrsanalysen entwickelt, dieses sei allerdings nicht im Geschäftsverkehr umgesetzt worden. Auf Nachfrage hat die Firma jedoch eingeräumt, man habe über einen Zeitraum von ca. 2 Monaten von der Muttergesellschaft Easycash GmbH Transaktionsdaten aus dem bargeldlosen Zahlungsverkehr zur Erstellung einer Zahlungsverkehrsanalyse für einen Geschäftskunden erhalten. Es habe sich dabei jedoch um pseudonymisierte Datensätze gehandelt, so dass keine Datenschutzverstöße vorlägen.

Dieser Darstellung widersprachen Erkenntnisse, die die Datenschutzaufsichtsbehörde in Nordrhein-Westfalen anlässlich einer zeitgleichen Überprüfung der Easycash GmbH in Ratingen erlangt hatte. Hiernach hat eine Übermittlung nicht verschlüsselter Transaktionsdaten aus dem EC-Lastschriftverfahren durch das Unternehmen an die Hamburger Tochtergesellschaft stattgefunden, gegen die der nordrhein-westfälische Datenschutzbeauftragte Strafantrag gestellt hat.

Wegen des Verdachts einer vorsätzlichen unbefugten Verarbeitung von personenbezogenen Daten mit Bereicherungsabsicht zumindest in einem Fall haben wir gegen die Easycash Loyalty Solutions GmbH Strafanzeige bei der Staatsanwaltschaft Hamburg gestellt. Nach unserer Auffassung dokumentierte das Geschäftsmodell der Easycash Loyalty Solutions GmbH eine Außerachtlassung wesentlicher Grundsätze des Datenschutzes, da es vorsah, Zahlungsanalysen über Kunden durch die Zusammenführung von Daten aus dem bargeldlosen Zahlungsverkehr mit Daten von Kundenkarten als „kostengünstiges Substitut zur Marktforschung“ gegen Entgelt zu erstellen.

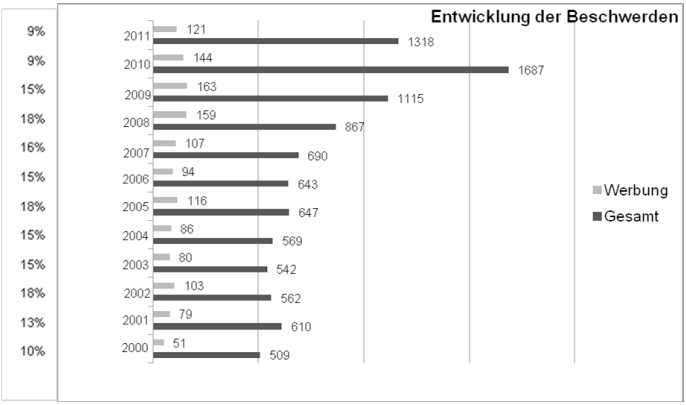
Die Ermittlungen der Staatsanwaltschaft haben ergeben, dass die Easycash GmbH aus Ratingen unberechtigt personenbezogene Daten, nämlich Transaktionsdaten aus EC-Karten-Umsätzen eines Händlers, an die Easycash Loyalty Solutions GmbH in Hamburg übermittelt hat. Die Easycash Loaylty Solutions GmbH habe diese Daten anonymisiert und die daraus gewonnenen statistischen Daten an den Kunden verkauft. Der Empfang der Daten durch die Easycash Loyalty Solutions GmbH stelle eine unbefugt vorgenommene Datenerhebung im Sinne des § 43 Abs. 2 Nr. 1 BDSG dar. Nach Auffassung der Staatsanwaltschaft handelte das Unternehmen in der Absicht, sich oder einen anderen zu bereichern. Dabei sei es nicht erforderlich, dass der erstrebte Vermögensvorteil rechtwidrig sei. Es reiche aus, dass aus der Tat Vorteile geschlagen würden. Das Verfahren gegen den zum Zeitpunkt der unbefugten Datenerhebung zuständigen Geschäftsführer des Hamburger Unternehmens wurde gegen Zahlung einer Geldbuße in Höhe von 50.000 Euro gem. § 153 a Strafprozessordnung eingestellt.

9. Werbung

9.1 Entwicklung der Beschwerden nach der Novellierung des Bundesdatenschutzgesetzes 2009

Die Beschwerden im Bereich Werbung und Adresshandel gehen zurück.

Bis zur Novellierung des Bundesdatenschutzgesetzes im Jahr 2009 war das Hauptanliegen der Bürger, die Herkunft ihrer Adressen, die zu Werbezwecken genutzt wurden, zu erfahren. Aufgrund der teilweise nicht umgesetzten, schon nach altem Recht geltenden Informationspflichten (vgl. IV 9.2), stieg der Umfang der Beschwerden teilweise auf bis zu 18% der gesamten schriftlichen Eingaben an. Im Berichtszeitraum ist nun ein leichter Rückgang zu verzeichnen:



Die Statistik der Jahre 2010 und 2011 macht deutlich, dass die Regelungen nach der Novellierung des Bundesdatenschutzgesetzes bei der Nutzung zum Zwecke der Werbung und des Adresshandels zwar immer noch einige Fragen aufwerfen, dennoch sind die Eingaben im Verhältnis zu den gesamten Eingaben rückläufig. Die absoluten Zahlen der Beschwerden haben sich im Vergleich zu den anderen Jahren allerdings nicht so gravierend verringert. Ursächlich dafür sind auch die nicht ganz einfachen gesetzlichen Regelungen (vgl. 9.2). Oft steht die Beratung über die Rechtslage im Vordergrund, da viele Personen nach wie vor davon ausgehen, dass personenbezogene Daten nur mit Einwilligung zu Werbezwecken genutzt oder übermittelt werden können (vgl. 22. TB IV 8.1).

Wir werden die weitere Entwicklung beobachten.

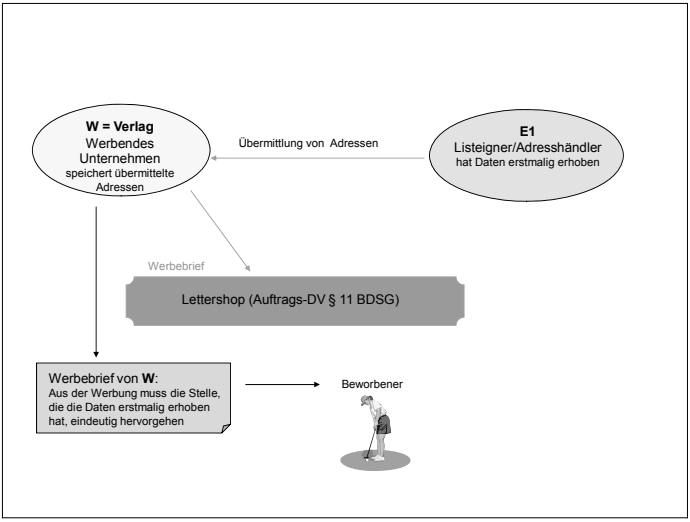
9.2 Hinweise zur Herkunft der Daten bei der Ansprache zu Werbezwecken

Nach wie vor bestehen Mängel bei der Angabe zur Herkunft im Werbeschreiben.

Die eingehenden Beschwerden zeigen, dass vielfach bei den werbenden Unternehmen oder bei den für die Datenverarbeitung verantwortlichen Stellen nicht bekannt ist, dass das Bundesdatenschutzgesetz Informationspflichten bei personalisierten Werbeaktionen festlegt. Dabei kommt es nicht darauf an, ob per Brief, Newsletter/E-Mail oder Telefon geworben wird. Bei der Ansprache zur Werbung ist der Betroffene neben dem Widerspruchsrecht über die Identität der verantwortlichen Stelle zu unterrichten. Nicht bewusst ist vielen Unternehmen, dass diese Regelung bereits seit der Novellierung des BDSG im Jahr 2001 gilt (§ 28 Abs. 4 Satz 2 BDSG).

Ebenfalls seit 10 Jahren sind die werbenden Unternehmen verpflichtet sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann, wenn personenbezogene Daten genutzt werden und die speichernde Stelle dem Werbenden nicht bekannt ist. Seit 2009 sind zusätzliche Regelungen zur Bekanntgabe der Herkunft geschaffen worden:

> Übermittlung nach § 28 Abs. 3 S. 4 BDSG
>
> Zusammengefasste personenbezogene Daten nach Satz 2 dürfen auch dann für Zwecke der Werbung übermittelt werden, wenn die Übermittlung nach Maßgabe des § 34 Absatz 1a Satz 1 gespeichert wird; in diesem Fall muss die Stelle, die die Daten erstmalig erhoben hat, aus der Werbung eindeutig hervorgehen.



Nutzung nach § 28 Abs. 3 S. 5 BDSG

Unabhängig vom Vorliegen der Voraussetzungen des Satzes 2 dürfen personenbezogene Daten für Zwecke der Werbung für fremde Angebote genutzt werden, wenn für den Betroffenen bei der Ansprache zum Zwecke der Werbung die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar ist.

Somit müsste jede Ansprache zur Werbung präzise Hinweise zur Herkunft enthalten. Die zahlreichen Auskunftsverlangen der Betroffenen zeigen jedoch, dass auch nach mehr als 2 Jahren vielfach die Informationen zur Herkunft fehlen oder ungenau sind. Es reicht nicht, nur auf Partnerunternehmen, Kooperationspartner oder eine öffentliche Quelle zu verweisen. Das Auskunftsrecht umfasst die Nennung des Namens mit Anschrift oder die genaue Bezeichnung der öffentlichen Quelle, damit der Betroffene seine Datenschutzrechte bei diesen Unternehmen wahrnehmen oder die Rechtmäßigkeit der Verwendung überprüfen kann.

9.3 Auskunftsverlangen nach § 34 BDSG nach dem Versand von Werbeschreiben

Wie „Sand im Getriebe" zu Schwierigkeiten bei den Auskunftsverlangen der Betroffenen führen kann.

Viele Betroffene gehen davon aus, dass ohne eine Einwilligung ihre Daten nicht zu Werbezwecken genutzt oder übermittelt werden dürfen. Da der Gesetzgeber jedoch Ausnahmen geschaffen hat (vgl. 22. TB, IV 8.1) und diese vielfach unbekannt sind, führt dies weiterhin zu Auskunftsersuchen bei den werbenden Stellen, gerade wenn die Herkunft der Adressdaten in der Werbemaßnahme nicht genannt wurde (vgl. IV 9.2). Sofern innerhalb einer angemessenen Frist, auch nach einer Erinnerung, nicht oder nur unzureichend reagiert wird, beschweren sich die Betroffenen bei der Aufsichtsbehörde für den Datenschutz. Bei den sich daran anschließenden Prüfungen konnten wir feststellen, dass

- erklärt wurde, die Auskunftsersuchen seien nicht eingegangen,
- Auskünfte unvollständig erteilt wurden:
  - o keine Nennung der Herkunft aus „Datenschutzgründen",
  - o allgemeine Beschreibung der Datenquelle,
  - o Nennung der Quelle ohne Anschrift,
  - o nur Mitteilung von Feldnamen oder Datenkategorien, keine Angabe der tatsächlich gespeicherten Daten,
  - o keine Aussage über Empfänger oder Empfängerkategorien,
  - o Datenlöschung bestätigt, ohne Auskunft zu erteilen.

Bei der Ermittlung des Sachverhaltes ist häufig aufgefallen, dass nicht die betrieblichen Datenschutzbeauftragten das Auskunftsersuchen bearbeitet hatten, sondern andere Organisationseinheiten im Unternehmen wie beispielsweise Kundencenter. Oftmals ist im Unternehmen nicht klar, wer solche Anfragen verantwortlich bearbeitet.

Ordnungswidrig handelt, wer fahrlässig oder vorsätzlich eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt (§ 43 bs. 1 Nr. 8a BDSG).

Die seit 2010 geltenden neuen Bußgeldtatbestände sollten Unternehmen dazu veranlassen, auf eindeutige Bearbeitungsregeln zu achten, um die Einleitung eines Bußgeldverfahrens zu vermeiden.

9.4 Telefonanrufe angeblicher Datenschutzeinrichtungen

Vorsicht vor vermeintlichen Datenschutz-Beratern am Telefon

In den vergangenen Monaten haben Bürgerinnen und Bürger verstärkt Anrufe erhalten, bei denen sich die Anrufer mit „Datenschutz Hamburg“, „Bundesdatenschutz Hamburg“, „Aktion Datenschutz“ oder „Datenschutzzentrale Hamburg“ vorstellten. Hierbei handelt es sich um Betrüger, die versuchen, dem Angerufenen Kontodaten zu entlocken oder angeblichen Datenschutz gegen Bezahlung anzubieten. Entweder wird um Vorauszahlung für Datenschutzleistungen gebeten oder der Angerufene soll dem Postboten 79,95 Euro oder einen anderen Betrag mitgeben, um dafür einen Gutschein über beispielsweise 700 Euro zu erhalten.

Eine neue Qualität erreichten diese betrügerischen Anrufe nicht nur dadurch, dass auf dem Display des Angerufenen eine Telefonnummer erscheint, die der des Hamburgischen Datenschutzbeauftragten täuschend ähnlich ist, es wurde auch der Name einer Mitarbeiterin des Datenschutzbeauftragten benutzt.

Die Anrufer erwecken den Anschein, von einer Behörde anzurufen. Eine Datenschutz-Aufsichtsbehörde würde niemals anrufen und Kontodaten erfragen. Auch bieten Datenschutzbehörden keinen Datenschutz gegen Entgelt an.

Wir empfehlen:

Nicht auf die Angebote dieser Anrufer eingehen, keinesfalls die Kontonummer angeben und das Gespräch umgehend beenden. Teilweise sind die Kontonummern dem Anrufer sogar bereits bekannt. In diesem Fall sollten regelmäßig die Kontobewegungen kontrolliert und auf unberechtigte Abbuchungen geachtet werden. Sind Lastschriften erfolgt, sollte diesen beim kontoführenden Kreditinstitut umgehend widersprochen werden.

10. Arbeitnehmerdatenschutz

10.1 Beschäftigtendatenschutzgesetz

Umfassendere gesetzliche Regelung des Beschäftigtendatenschutzes in Sicht?

Zum 1. September 2009 ist mit § 32 eine besondere Regelung in das Bundesdatenschutzgesetz eingefügt worden, welche die Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

zum Inhalt hat. Die neue Bestimmung lässt jedoch eine Reihe dringender Fragen des Arbeitnehmerdatenschutzes offen.

Mittlerweile hat die Bundesregierung einen Gesetzentwurf in den Bundestag eingebracht, der sich noch in der Beratung der parlamentarischen Gremien befindet. In einer Arbeitsgruppe haben sich Aufsichtsbehörden sowie Datenschutzbeauftragte des Bundes und der Länder mit dem Gesetzentwurf befasst und Stellungnahmen erarbeitet:

- Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22. Juni 2010
- Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2011.

Wir begrüßen, dass nunmehr jahrzehntelangen Forderungen der Datenschutzbeauftragten Rechnung getragen wird und eine umfassendere gesetzliche Regelung des Beschäftigtendatenschutzes erfolgen soll (vgl. 22. TB, IV 9.2). Derzeit ist allerdings nicht absehbar, wann das Gesetzgebungsverfahren beendet sein wird. Wir werden die weitere Debatte aufmerksam verfolgen.

11. Bußgeldfälle und Strafanträge

Die Anzahl der Datenschutzverstöße, die mit einem Bußgeld geahndet wurden, hat sich mehr als verdoppelt.

Im Vordergrund unserer aufsichtsbehördlichen Tätigkeit steht zwar nicht, Bußgelder zu verhängen. Allerdings führten im Berichtszeitraum wesentlich mehr Datenschutzverstöße zur Einleitung von insgesamt 13 Ordnungswidrigkeitenverfahren:

Tatbestand § 43 Abs. 1 Nr.	*Tatbestand § 43 Abs. 2 Nr.*	*Sachverhalt*	*Bußgeld in €*	*E = Einspruch N = Kein Einspruch*	*Verfahrens-ausgang vor dem Amtsgericht*
	1	Unbefugte Videoüberwachung von Kunden und Mitarbeitern in einer Bäckerei	1.500,00	E	Einspruch stattgegeben, Verfahren eingestellt
	1	Unbefugte Datenübermittlung an ärztliche Verrechnungsstellen ohne Einwilligung der Patienten	700,00	E	Einspruch zurück-genommen
2		Nichtbestellung eines betrieblichen Datenschutzbeauftragten	3.000,00	N	
	1 + 2	Bankdaten: Unbefugte Erstellung von Kundenprofilen (Neuromarketing), Zugriff für Kundenberater auf Kundendaten (vgl. IV, 7.1)	200.000,00	N	gezahlt
10		Nichterteilung einer Auskunft gegenüber der Aufsichtsbehörde	1.000,00	E	Reduzierung auf 500 €
10		Nichterteilung einer Auskunft gegenüber der Aufsichtsbehörde	1.000,00	E	noch offen
	1	Einholung von Auskünften bei einer Auskunftei über Bewerber vor Einstellung ohne Einwilligung des Betroffenen	700,00	N	gezahlt
10		Nichterteilung einer Auskunft gegenüber der Aufsichtsbehörde	1.000,00	E	Verfahren eingestellt
10		Nichterteilung einer Auskunft gegenüber der Aufsichtsbehörde	1.000,00	N	
1+5+8+8a	1	Unbefugtes Speichern + zur Verfügungstellen von bonitätsrelevanten Daten zum Abruf	7.000,00	E	noch offen
8a	1	Unbefugte Erhebung bei einer anderen Stelle des Unternehmensverbundes (Auskunfteitätigkeit)	5.000,00	N	gezahlt
10		Nichterteilung einer Auskunft gegenüber der Aufsichtsbehörde	500,00	N	
	3	Unbefugtes Abrufen von Bankdaten	300,00	N	

Die Aufsichtsbehörde stellte darüber hinaus im Berichtszeitraum 3 Strafanträge.

12. Meldepflicht und Prüftätigkeit

12.1 Meldepflicht nach § 42a BDSG

Viele Unsicherheiten bestehen bei den Unternehmen, ob sie Vorfälle melden müssen oder nicht.

Im Berichtszeitraum erreichten uns zahlreiche Meldungen über Datenschutzpannen. Oftmals waren sich die Unternehmen nicht sicher, ob der Vorfall der Aufsichtsbehörde zu melden war. Viele Meldungen wurden daher vorsorglich getätigt.

Seit September 2009 verpflichtet der neu eingefügte § 42 a BDSG die nicht-öffentliche Stelle zu unverzüglicher Mitteilung an die Aufsichtsbehörde und die Betroffenen unter folgenden Voraussetzungen:

- Wenn bei der nicht-öffentlichen Stelle gespeicherte
  - o besondere Arten personenbezogener Daten (rassische, ethnische Herkunft; politische Meinungen; religiöse, philosophische Überzeugungen; Gewerkschaftszugehörigkeit; Gesundheit; Sexualleben),
  - o personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
  - o personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten beziehen,
  - o personenbezogene Daten zu Bank- oder Kreditkartenkonten
- unrechtmäßig übermittelt oder
- auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind

und

dadurch schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

Die Informationspflicht nach § 42 a BDSG soll den Betroffenen vor weiteren Schäden durch möglichen Missbrauch seiner Daten schützen. Soweit die Benachrichtigung der Betroffenen – insbesondere aufgrund der Vielzahl der betroffenen Fälle – einen unverhältnismäßigen Aufwand darstellt, ist stattdessen die Information der Öffentlichkeit durch halbseitige Anzeigen in zwei bundesweit erscheinenden Tageszeitungen vorgesehen.

Seit Einführung dieser Meldepflicht sind 21 Anzeigen eingegangen. In 9 Fällen lag tatsächlich eine Meldepflicht vor. Beispielhaft sind einige Vorfälle nachstehend beschrieben:

Anlass der Meldung	Informationspflicht bejaht/verneint
Reederei, versehentliche Übermittlung von Kreditkartendaten an 43 Reisende durch einen Dienstleister.	ja
Verein wegen Diebstahls eines Datenträgers mit Mitgliederdaten.	ja
Reiseveranstalter (5. Februar 2010) wegen Entwendung von 3 Laptops durch einen Einbruch. Darauf befanden sich Kundendaten, die durch Passwort gesichert sind.	ja
Handelsunternehmen wegen Übermittlung von Mitarbeiterkontodaten aufgrund Fehlers eines Mitarbeiters des Dienstleisters (Vertauschen von Seiten von Anschreiben).	ja
Verlag wegen Zugriff auf Abonenntendaten.	ja
Versicherungsvermittler wegen Diebstahls eines Laptops mit 2010 Versicherungsnehmerdaten.	ja
Verlag wegen Diebstahls einer Paketsendung bei Kurier durch Einbruch in ein Lager eines Subunternehmers (Mitarbeiterdaten).	ja
Verlag wegen evtl. Missbrauchs von E-Mail-Adressen von Kunden durch Mitarbeiter oder Dritte.	nein
Hacken einer Internet-Seite eines Verlages und Zugriff auf personenbezogene Daten durch Studenten.	ja
Produzierendes Gewerbe: Diebstahl eines passwortgeschützten Laptops einer Führungskraft, in dessen lokal gespeichertem Adressbuch sowie dessen lokal gespeichertem E-Mail-Verkehr sich personenbezogene Daten (insbesondere Bewerber-Daten) befunden haben.	nein
Manipulation eines EC-Zahlungs-Terminals bei einem Einzelhändler	ja
Hacking-Angriff auf die Internetseite eines Einzelhändlers. Dadurch Zugriff auf Kundendaten und Daten von Gewinnspielteilnehmern. Nach Darstellung des Unternehmens waren keine Kontodaten betroffen.	nein

Hilfestellung zur Prüfung nach § 42 a BDSG unter

www.datenschutz-berlin.de/content/themen-a-z/informationspflicht-nach-42-a-bdsg

Weitgehend unbemerkt geblieben ist die Mitteilungspflicht nach § 83a SGB X. Seit 11. August 2010 sind Sozialleistungsträger ebenso verpflichtet, Datenschutzvorfälle zu melden, wenn gespeicherte besondere Arten personenbezogener Daten

- unrechtmäßig übermittelt oder
- auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind

und

dadurch schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

Der Aufsichtsbehörde wurden bisher 3 Fälle gemeldet.

12.2 Register

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.

> § 4d Abs. 4 BDSG:
>
> Meldepflicht gilt für automatisierte Verarbeitungen, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle
>
> 1. zum Zweck der Übermittlung,
>
> 2. zum Zweck der anonymisierten Übermittlung oder
>
> 3. für Zwecke der Markt- oder Meinungsforschung
>
> gespeichert werden.

51 Unternehmen sind entsprechend den Vorgaben des § 4e BDSG zum Register gemeldet (vgl. 18. TB, 29.1, 19. TB, 27.1, 20. TB 30.1, 21. TB, 30.1, 22. TB 11.1). Unterteilt nach der Art der meldepflichtigen Verfahren ergibt sich folgendes Bild:

- Speicherung zum Zwecke der Übermittlung

Auskunfteien/Warndienste	12
Informationsdienste	4
Adresshändler	9

- Speicherung zum Zwecke der anonymisierten Übermittlung oder für Zwecke der Markt- und Meinungsforschung 26

12.3 Prüfungsprogramm der Dienststelle: „Intelligente Steuerung im nicht-öffentlichen Bereich“

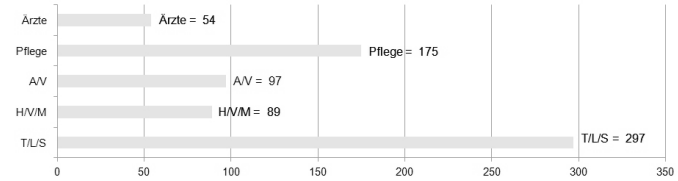
Ein selbstverantwortliches Datenschutzmanagement im Dienst von Kunden, Verbrauchern und Mitarbeitern kann im Wettbewerb helfen.

Wir haben im Januar 2010 eine Fragebogenaktion bei Hamburger Unternehmen mit dem Ziel begonnen, die Bedeutung der betrieblichen Datenschutzbeauftragten in den Unternehmen zu stärken und dort, wo trotz gesetzlicher Verpflichtung keine betrieblichen Datenschutzbeauftragten benannt sind, deren zeitnahe Bestellung zu erwirken. Nach § 4f Abs. 1 BDSG müssen Unternehmen, bei denen mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, einen betrieblichen Datenschutzbeauftragten bestellen.

Grund für diese Aktion waren die zahlreichen Datenpannen und Datenmissbräuche der letzten Jahre, mit denen Unternehmen ganz unterschiedlicher Branchen in das Licht der Öffentlichkeit gerieten und die ein erschreckendes Defizit an Professionalität im Umgang mit dem Datenschutz und der Datensicherheit dokumentierten. Zudem erweist sich, dass das Instrument des betrieblichen Datenschutzbeauftragten als Scharnier zwischen betrieblicher Eigenverantwortlichkeit und der Wahrung des informationellen Selbstbestimmungsrechts des Betroffenen fungiert. Die Befragungsaktion war daher eine Maßnahme, die in Zusammenhang mit dem Konzept Hamburger Datenschutz 2010 künftig die innerbetrieblichen Steuerungspotentiale aufwerten sollte.

Um durch die Aktion möglichst viele Unternehmen gleichzeitig zu erreichen, wurde ein schriftliches Prüfungskonzept erarbeitet, das sich auf die Person und Fachkunde des betrieblichen Datenschutzbeauftragten in den Unternehmen konzentrierte:

Es wurden 712 Unternehmen nach einem betrieblichen Datenschutzbeauftragten befragt.



T/L/S = Transport/Logistik/Spedition
H/V/M = Haus- und Immobilienverwalter und –makler
A/V = Arbeitsvermittler/Zeitarbeitsfirmen
Pflege = Pflegedienste
Ärzte = ärztliche Gemeinschaftspraxen

Die Auswertung der Fragebogenantworten ergab, dass der weitaus größte Teil der bestellpflichtigen Unternehmen einen betrieblichen Datenschutzbeauftragten hatte. In einigen Fällen hatten die Unternehmen die Bestellpflicht nicht beachtet und mussten nachträglich betriebliche Datenschutzbeauftragte bestellen. Die von der Aufsichtsbehörde durchgeführten Stichproben ergaben, dass die Datenschutzbeauftragten allerdings nicht in allen Fällen die erforderliche Sach- und Fachkunde vorweisen konnten. In der Spitze lag die Misserfolgsquote (keine Bestellung sowie keine Fachkunde vorhanden) bei 10%.

Ergebnisse der Fragebogenaktion 2010
Absolute Zahlen

	Gesamt	bestellt	keine Bestellpflicht	müssen bestellen
An Firmen versandte Fragebögen:	**712**			
Transport/Logistik/Spedition	**297**	**240**	**54**	**3**
Haus- und Immobilienverwalter und –Makler	**89**	**52**	**28**	**9**
Arbeitsvermittler/Zeitarbeitsfirmen	**97**	**48**	**46**	**3**
Pflegedienste:	**175**	**135**	**36**	**4**
Ärztliche Gemeinschaftspraxen:	**54**	**29**	**22**	**3**

Fehlende Fachkunde:	
Transport/Logistik/Spedition	**7 Firmen**
Haus- und Immobilienverwalter und –makler	**2 Firmen**

Im Zuge der zur Nachkontrolle durchgeführten Stichproben vor Ort bei den Unternehmen der Branchen Zeitarbeit, Pflege sowie Hausmakler, die angeblich keiner Bestellpflicht unterlagen, ergab sich, dass entgegen der eigenen Angaben die Mindestzahl erreicht und somit eine Bestellung im Einzelfall vorzunehmen war. Darüber hinaus erweiterten wir den Fragenkatalog. Es zeigte sich, dass bei den Unternehmen, die bereits bei der Umsetzung der Bestellpflicht Probleme hatten, auch andere datenschutzrechtliche Mängel auftraten.

Folgende Mängel haben wir festgestellt und entsprechende Forderungen erhoben:

Ergebnisse der vor Ort-Prüfung 2011
Absolute Zahlen

	Gesamt
Vor Ort geprüfte Firmen:	15
Haus- und Immobilienverwalter und –Makler	5
Arbeitsvermittler/Zeitarbeitsfirmen	5
Pflegedienste:	5
Forderungen:	
Datenschutzbeauftragter muss bestellt werden :	11
Dienstleistungsvertrag mit Auftragsdatenverarbeitern fehlt :	12
Verfahrensbeschreibung fehlt :	12
Verpflichtungserklärung nach § 5 BDSG fehlt :	12
Passwortkonventionen nicht eingehalten:	7

Der bisherige Verlauf der Aktion kann sich für die Hamburgische Wirtschaft aber durchaus sehen lassen: Die überwiegende Beachtung der Bestellpflicht der Beauftragten ist ein Indiz dafür, dass sich der Umgang mit dem Datenschutz und der Datensicherheit in den Unternehmen verbessert hat. Die Einsicht, dass ein selbstverantwortliches Datenschutzmanagement im Dienst von Kunden und Verbrauchern auch im Wettbewerb helfen kann, scheint sich durchzusetzen. Langfristig bleibt es unser Ziel, die betrieblichen Datenschutzbeauftragten in den Unternehmen künftig auch in die Bearbeitung von Bürgerbeschwerden mit einzubeziehen.

Wir werden dennoch unser Prüfungsprogramm fortsetzen.

Dienststelle (Stand: 1. Februar 2012)

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Tel: 040/42854-4040

Klosterwall 6, 20095 Hamburg Fax: 040/42841-4000

E-Mail: mailbox@datenschutz.hamburg.de

Internet-Adresse: www.datenschutz-hamburg.de

		Durchwahl
Dienststellenleiter:	Prof. Dr. Johannes Caspar	-4040-
Stellvertreter:	Herr Dr. Menzel	-4049-
Vorzimmer:	Frau Niemann	-4040-
Geschäftsleiter, Presse- und Medienreferent Herr Gerhards		-4153-
Verwaltungsleiter Herr Nentwig		-4043-
Vorzimmer, Geschäftsstelle Frau Niemann		-4040-
Registratur, Geschäftsstelle Frau Schmidt		-4042-
IT-Leiter, Internet, Öffentlichkeitsarbeit Herr Schemm		-4044-
Öffentlichkeitsarbeit Herr Krenz		-4142-
E-Government, technisch-organisatorische Beratung und Prüfung Herr Dr. Wirth		-4053-
Netzwerke, Biometrie, technisch-organisatorische Beratung und Prüfung Herr Kühn		-4054-
Dokumentenmanagement/Archivierung, Videoüberwachungstechnik, technisch-organisatorische Beratung und Prüfung Frau Nadler		-4055-

Soziale Netzwerke, technisch-organisatorische Beratung und Prüfung
Herr Schneider -4061-

Elektronischer Rechtsverkehr, technisch-organisatorische Beratung und Prüfung
Herr Morische -4048-

SAP, anlassfreie Unternehmensprüfung
Herr Mielke -4045-

Informationsfreiheit
Frau Dr. Thomsen -4062-

Informationsfreiheit, Modernisierung des Datenschutzrechts
Herr Dr. Schnabel -4047-

Informationsfreiheit, Soziale Netzwerke, Vereine, Freie Berufe
Herr Dr. Karg -4051-

Gesundheitswesen, Justiz, Staatsanwaltschaft, verfassungsschutz, Strafvollzug, Bauen und Wohnen, Umwelt, Kultur, Forschung, Archivwesen
Herr Dr. Menzel -4049-

Ausländerwesen, Wirtschaftsverwaltung, Gewerberecht, Hochschulwesen Straßenverkehrsverwaltung, Wahlen und Volksabstimmungen, Waffenrecht
Frau Scheffler -4064-

Polizei, Rundfunk, Medien (GEZ)
Frau Wolters -4052-

Soziales, Schulwesen, Kinderbetreuung, Allgemeine Bezirksangelegenheiten, Finanz-, Steuer- und Rechnungswesen, Feuerwehr, Kirchen
Herr Malessa -4050-

Statistik, Personenstandswesen, Meldewesen, Ausweis- und Passangelegenheiten
Frau Kranold -4046-

Videoüberwachung im öffentlichen Bereich
Herr Vetters -4147-

Auskunfteien, SCHUFA, Internationaler Datenverkehr, Telemedien
Frau Naujok -4058-

Stichwortverzeichnis

Anlage 2

DATENSCHUTZ
FAKTEN ZAHLEN DATEN

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

HmbBfDI

Hamburg

Jede Person kann sich an die Hamburgische Beauftragte bzw. den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit wenden, wenn sie der Ansicht ist, bei der Verarbeitung ihrer personenbezogenen Daten (…) in ihren Rechten verletzt worden zu sein.
§ 26 Absatz 1 HmbDSG
(Hamburgisches Datenschutzgesetz)

Zu den Aufgaben des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) gehört es, sich für die Bürgerinnen und Bürger stark zu machen – gerade in Angelegenheiten, in denen sie aus eigenen Kräften nichts erreicht haben oder keine Möglichkeiten mehr sehen, ihre Rechte aussichtsreich selbst zu vertreten. In vielen Fällen kann den Beschwerden abgeholfen werden, weil Unternehmen, aber auch Behörden anders reagieren, wenn der Datenschutzbeauftragte „auf der Matte steht".

Die Eingaben von Bürgerinnen und Bürgern machen - neben der Beratung privater und öffentlicher Stellen - einen großen Teil unserer täglichen Arbeit aus. Mal sind es relativ einfache Fälle, die schnell erledigt sind. Oft sind die Beschwerden aber auch Auslöser für langwierige und aufwändige Prüfungsverfahren. Sie enden dann mitunter auch mit einem Bußgeld oder vor Gericht. Dabei helfen die Eingaben nicht nur den Beschwerdeführerinnen und Beschwerdeführern. Sie machen uns auf Missstände aufmerksam, die wir sonst eventuell gar nicht bemerkt hätten.

Auf den folgenden Seiten stellen wir losgelöst von unserem Tätigkeitsbericht 2010/2011 unsere Eingabenstatistik der vergangenen Jahre vor. Diese belegt einen Anstieg der Eingaben über die Jahre hinweg und dokumentiert über Hamburg hinaus die wachsende Bedeutung des Datenschutzes in der digitalen Gesellschaft. Während die Beschwerden gegen öffentliche Stellen nahezu konstant geblieben sind, steigen die Beschwerden gegen private Unternehmen insbesondere im Bereich Internet-Dienstleistungen an. Die Bedrohungslage scheint sich mit zu verschieben: „vom Überwachungsstaat zur Überwachungsgesellschaft" (Prof. Dr. Johannes Caspar).

So viele Eingaben wie noch nie!

In den Jahren 2010 und 2011, also dem Berichtszeitraum des 23. Tätigkeitsberichts, haben sich **2.901 Bürgerinnen und Bürger** mit Eingaben per Post oder per E-Mail an uns gewandt. In dieser Zahl sind die vielen telefonischen Anfragen und Beschwerden nicht erfasst. Außerdem wurden für diese Informationsbroschüre 122 Eingaben nicht einberechnet, die wir nach Prüfung der Zuständigkeit an andere Datenschutzbeauftragte abgeben mussten. Trotzdem sind es insgesamt fast 1.000 Eingaben mehr als in den Jahren 2008 und 2009. Das entspricht einer Steigerung von 46%.

Welche Branchen bzw. Verwaltungsbereiche wie oft betroffen waren, zeigt die umseitige Tabelle. Darin wird zwischen Eingaben, die sich auf den nicht-öffentlichen Bereich (Datenschutzverstöße von Firmen und Unternehmen) und Eingaben, die sich auf den öffentlichen Bereich (Datenschutzverstöße von Behörden und anderen Einrichtungen der Stadt Hamburg) beziehen, unterschieden.

Auch im Berichtszeitraum 2010/2011 bestätigt sich wieder der Trend, dass die Eingaben von Bürgerinnen und Bürgern beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit ansteigen. Besonders deutlich wird dieser Trend, wenn man die Anzahl der Eingaben der vergangenen 10 Jahre vergleicht.

Der Hamburgische Datenschutzbeauftragte ist datenschutzrechtliche Aufsichtsbehörde für 160.000 in Hamburg ansässige Handelsunternehmen.
(Quelle: Handelskammer Hamburg)

Der signifikante Anstieg im Jahr 2010 ist auch auf das bundesweit durch den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit koordinierte Widerspruchsverfahren zu Google Street View zurückzuführen.

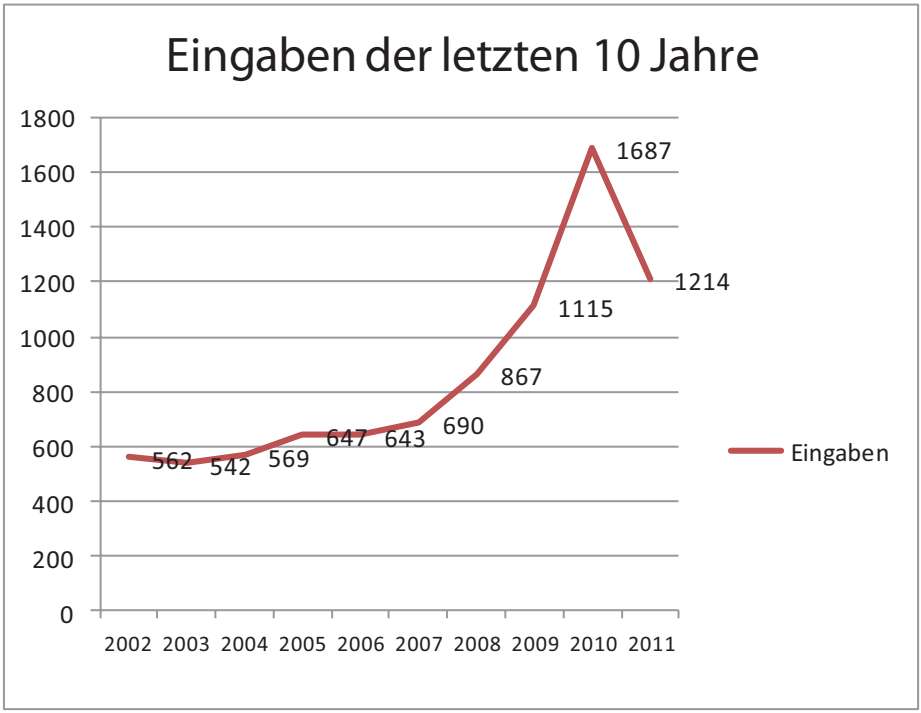


Abbildung 1: Entwicklung der Eingaben 2002 - 2011

Auch für die über 20 Hamburger Hochschulen mit ihren ca. 80.000 Studentinnen und Studenten sowie für die 500 allgemein- und berufsbildenden Schulen mit rund 250.000 Schülerinnen und Schülern ist der HmbBfDI in Fragen des Datenschutzes zuständig.

Eingaben 2010/2011

Branche / Verwaltungsbereich	2010	2011
Adresshandel	35	17
Auskunfteien	69	54
freie Berufe	38	26
Gastronomie	13	2
Gewerbliche Dienstleistungen	50	82
Handel allgemein	98	80
Heime	3	1
Hochschule, nicht-öffentlich	1	3
Inkassounternehmen	20	14
Krankenhäuser	1	6
Kreditwirtschaft	43	34
Markt- und Meinungsforschung	2	6
Soziales und Gesundheitswesen, nicht-öffentlich	41	40
Telekommunikation	53	47
Tele- und Mediendienste	742	335
Versandhandel	31	29
Versicherungswirtschaft	31	16
Wohnungswirtschaft, privat	33	25
Vereine, Parteien	23	30
Öffentlicher Nahverkehr und Verkehrswesen	15	19
Verlage	37	23
Sonstiges, nicht-öffentlich	1	105
Allgem. Bezirksangelegenheit	5	3
andere Sozialbereiche	18	10
Arbeitslosengeld II	30	5
Ausländerwesen	2	4
Bau- und Vermessungswesen	1	3
Bildungswesen	19	27
Feuerwehr	1	0
Gesundheitswesen öff.	15	19
Hochschulwesen	10	3
Justiz	11	14
Kinder- und Jugendhilfe	2	2
Kultur	2	1
Medizinscher Dienst d. KV MDK	3	5
Parlamentswesen/Bezirksvers.	0	0
Pass - und Meldewesen	19	14
Personenstandswesen	3	0
Polizei	23	18
Sozialhilfe	1	5
Sozialversicherung	2	8
Staatsanwaltschaft	9	2
Statistik	3	30
Steuern und Abgaben	8	12
Strafvollzug	11	8
Umweltschutz	1	0
Verfassungsschutz	1	0
Verkehrswesen öff.	9	3
Wahlen und Volksabstimmung	4	3
Wirtschaftsverwaltung	3	5
Sonstiges öff.	91	16
Gesamt:	1687	1214

Tabelle 1: Eingaben 2010/2011

Während die Eingaben der Bürgerinnen und Bürger ansteigen, bleibt die Personalausstattung der Datenschutzbehörde hinter dieser Entwicklung zurück. Am 31.12.2011 hatte der Hamburgische Datenschutzbeauftragte im Bereich Datenschutz und interner Verwaltung 17 Mitarbeiter, die sich auf 13,7 Stellen verteilten (14,7 Stellen, wenn der Datenschutzbeauftragte selbst mit einberechnet wird). Hinzu kamen 4 Kolleginnen und Kollegen (3,1 Stellen), die zeitlich befristet von anderen Dienststellen zum Datenschutzbeauftragten abgeordnet wurden. Ein Blick auf den 10-Jahres-Vergleich zeigt, dass der Personalbestand insgesamt zurückgegangen ist.

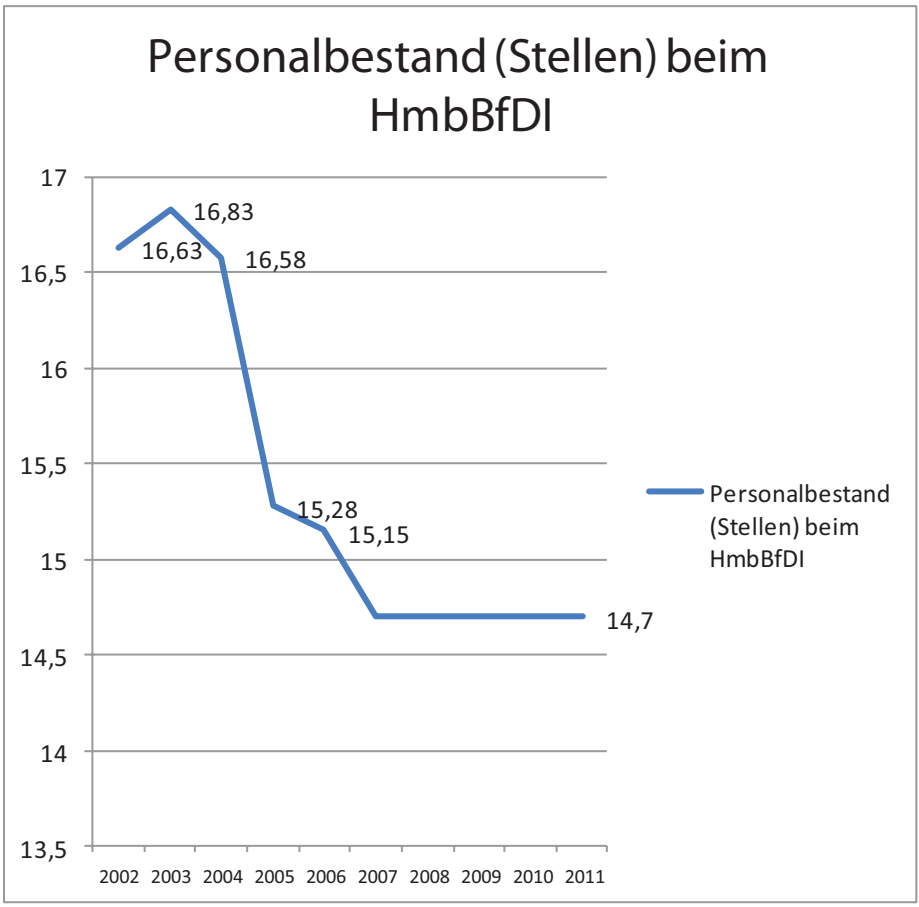


Abbildung 2: Entwicklung des Stellenbestands 2002 - 2011

Während die Zahl der Eingaben im Vergleich von 2002 und 2011 um etwa 54% gestiegen ist, ist im gleichen Zeitraum der Stellenbestand um rund 13% gesunken.

1.214 Eingaben pro Jahr klingt vielleicht nach nicht viel. Dabei muss man sich je nach Einzelfall aber vor Augen halten, dass die Bearbeitung von Eingaben mitunter sehr zeitintensiv und aufwändig sein kann. Die Eingaben machen zudem nur einen Teil der Arbeit des Datenschutzbeauftragten aus. Hinzu kommen Beratungen von Bürgerinnen und Bürgern, aber auch von behördlichen und betrieblichen Datenschutzbeauftragten, rechtliche und technische Prüfungen, die Begleitung von IT-Projekten der Hamburger Verwaltung, Stellungnahmen zu Gesetzesvorhaben, die Teilnahme an bundesweiten Arbeitskreisen und nicht zuletzt die Beantwortung von Fragen der nationalen und internationalen Presse.

In einem Vergleich der Personalausstattung der Datenschutzbeauftragten der Länder rangiert der HmbBfDI auf einem der letzten Plätze.

(Quelle: „XAMIT Datenschutzbarometer 2011"; verglichen wurde die Zahl des Kernpersonals von 14 Landesdatenschutzbeauftragten, der HmbBfDI liegt dabei an dreizehnter Stelle)

Ein Vergleich der Eingaben im öffentlichen Bereich mit denen im nichtöffentlichen Bereich macht deutlich, dass sich erheblich mehr Eingaben gegen private Unternehmen und Firmen richten als gegen Behörden. Dies ist ebenfalls Ausdruck einer seit den vergangenen 10 Jahren zu beobachtenden Tendenz. Während, wie bereits eingangs gesagt, die Eingaben im öffentlichen Bereich nur leichten Schwankungen unterworfen sind, steigen die Eingaben im nicht-öffentlichen Bereich stetig an.

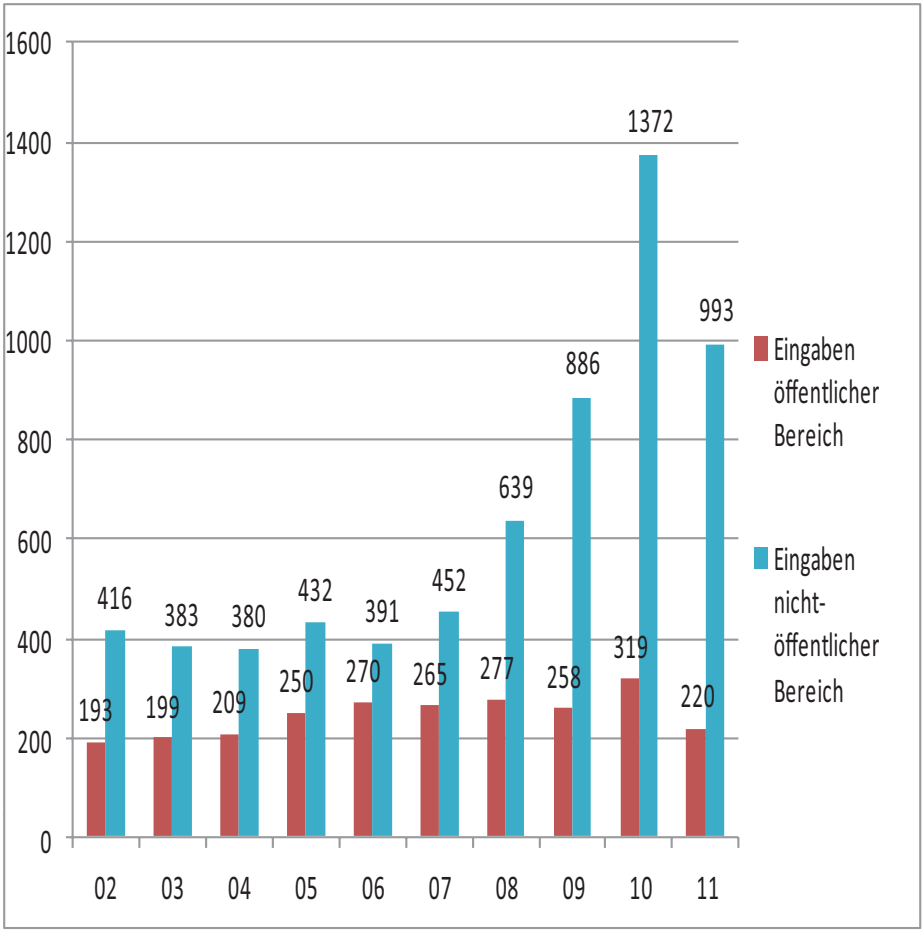


Abbildung 3: Eingaben im öffentlichen und im nicht-öffentlichen Bereich im 10-Jahres-Vergleich

Die gestiegene Zahl der Eingaben von Bürgerinnen und Bürgern im nicht-öffentlichen Bereich ist insbesondere auf die große Zahl der Eingaben zurückzuführen, die sich gegen Tele- und Mediendienste richten (siehe Tabelle 1).

Hinter dem Ausdruck Tele- und Mediendienste verbergen sich unter anderem Anbieter von Internetdiensten, also zum Beispiel auch Google und Facebook, die ihre deutsche Hauptniederlassung in Hamburg haben. Die Zahl der Beschwerden gegen solche Unternehmen steigt kontinuierlich an, gerade wenn es sich um Firmen handelt, deren Geschäftszweck auf dem Sammeln von personenbezogenen Daten einer Nutzerinnen und Nutzer beruht.

Auch wenn man die einmalige „Street-View-Spitze“ des Jahres 2010 außer Acht lässt, ist bei den Eingaben, die sich in den letzten 10 Jahren gegen Tele– und Mediendienste richteten, ein klarer Trend erkennbar.

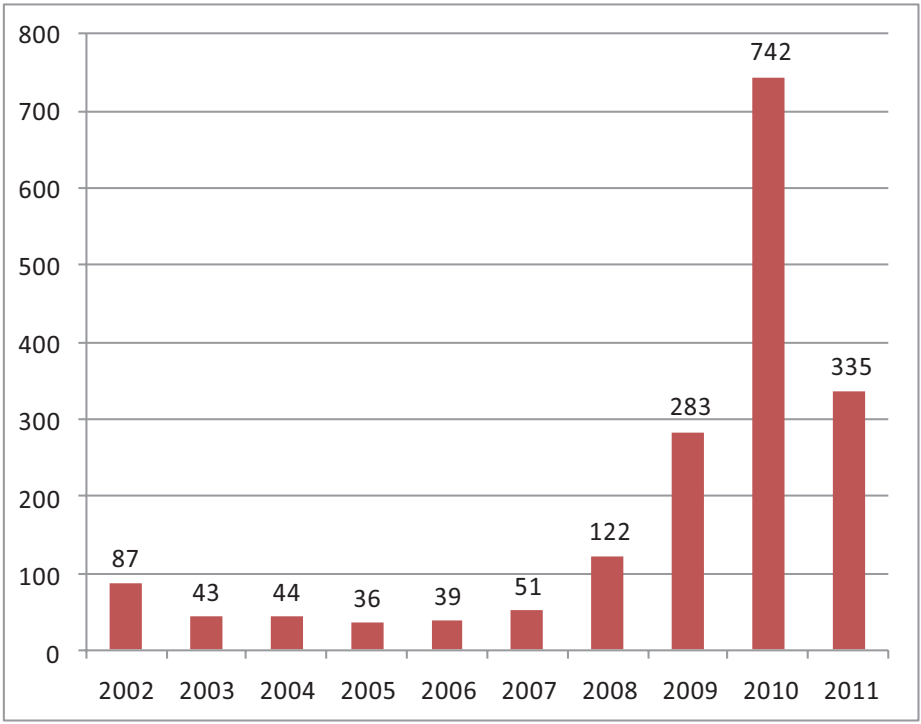


Abbildung 4: Eingaben „Tele- und Mediendienste“ 2002 - 2011

Facebook, Google und Xing haben ihren Deutschlandsitz in Hamburg, weitere internationale Internetanbieter sollen folgen.

Die Beschwerden über Datenschutzverstöße im Internet sind dabei nicht auf Tele- und Mediendienste beschränkt. Da mittlerweile jedes Geschäft seinen Onlineshop hat, jeder Verein seine Homepage und jedes Kreditinstitut Onlinebanking anbietet, sind von diesen Eingaben alle Branchen betroffen.

Eine Übersicht der Eingaben im nicht-öffentlichen Bereich nach Themen für den Zeitraum 2010/2011 zeigt, dass neben den sonstigen Themen (in der Grafik „Allgemein“ - Beschwerden, die keinem anderen Bereich zuzuordnen sind) das Internet die Hauptquelle für Beschwerden von Bürgerinnen und Bürgern war. Angesichts der gesellschaftlichen Entwicklung ist dies kein überraschendes Ergebnis.

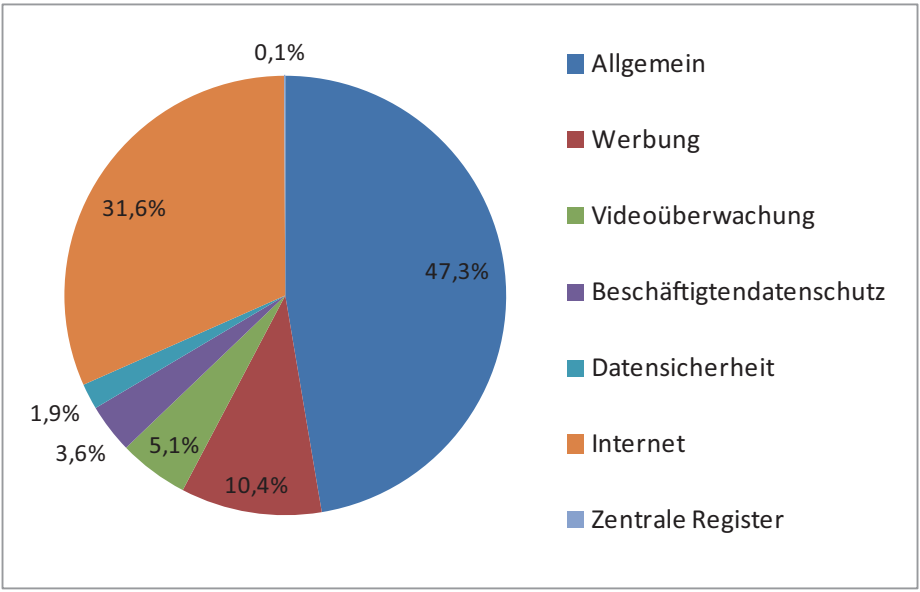


Abbildung 5: Eingaben 2010/2011 thematisch (nicht-öffentlicher Bereich)

Weitere statistisch erfasste Tätigkeiten der Dienststelle des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit für den Berichtszeitraum des 23. Tätigkeitsberichts:

Beratungen zu rechtlichen, technischen und organisatorischen Fragen			
öffentliche Stellen		nicht öffentliche Stellen	
2010	2011	2010	2011
721	579	540	457

Rechtliche und technische Prüfungen von Daten verarbeitenden Stellen, einschl. Softwaresysteme			
öffentliche Stellen		nicht-öffentliche Stellen	
2010	2011	2010	2011
360	338	234	184

Stellungnahmen zu Rechts- und Verwaltungsvorschriften	
2010	2011
71	76

Kontakt

Herausgeber:
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6
20095 Hamburg
Tel.: 040/42854-4040 (Geschäftsstelle)
Fax: 040/42854-4000
E-Mail: mailbox@datenschutz.hamburg.de

Layout: KAMEKO Design Gbr
Titelbild: Thomas Krenz
Druck: Print 74 - Schnakenberg- Druckerei und Verlagsgesellschaft mbH
Diese Publikation kann auch unter www.datenschutz-hamburg.de im PDF-Format heruntergeladen werden.

März 2012