# 32. Jahresbericht der Landesbeauftragten für Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats über das Ergebnis der Tätigkeit im Jahre 2009 den 32. Jahresbericht zum 31. März 2010 (§ 33 Abs. 1 Bremisches Datenschutzgesetz – BremDSG). Redaktionsschluss für die Beiträge war der 31. Dezember 2009.

Dr. Imke Sommer
Die Landesbeauftragte für Datenschutz und Informationsfreiheit

**Inhaltsverzeichnis**

## 1. Vorwort

Die Bremische Bürgerschaft hat mich am 29. April 2009 zur Landesbeauftragten für Datenschutz und Informationsfreiheit gewählt. Daher ist dies der erste Jahresbericht zum Datenschutz, den ich der Bremischen Bürgerschaft und dem Präsidenten des Senats der Freien Hansestadt Bremen vorlege. Diese Gelegenheit möchte ich nutzen, meinem Vorgänger Sven Holst, der dieses Amt in den ersten Monaten des Berichtszeitraumes ausfüllte, dafür zu danken, dass ich meine Arbeit in einer Dienststelle mit hoch motivierten Mitarbeiterinnen und Mitarbeitern aufnehmen konnte. Der gute Datenschutzruf, den Bremen bundesweit genießt, begünstigte auch meinen Start im Kreis meiner Kollegin und meiner Kollegen aus dem Bund und den anderen Ländern.

**Datenschutz als Menschenrechtsthermometer**

Die Menschenrechte sind kein Luxus, sondern die Basis unseres demokratischen Gemeinwesens. Dies gilt gerade in Zeiten, in denen eine wirtschaftlich schwierige Lage dazu verleitet, das gesellschaftliche Augenmerk allein auf die Überwindung dieser Situation zu lenken, und in denen deshalb das Aufrechterhalten errungener Standards in allen Bereichen schwierig wird. Dabei ist die Einhaltung dieser Standards gerade dann wichtig: Nur selbstbewusste Menschen, die sich wertgeschätzt fühlen und die ihre demokratischen Rechte kennen und nutzen, können die Kreativität und Tatkraft entfalten, die Wirtschaft und Gesellschaft benötigen, um Krisen zu bewältigen.

Zu diesen wichtigen Menschenrechten gehört auch das Grundrecht auf informationelle Selbstbestimmung. Es fußt auf der unabdingbaren Menschenwürde und dem Grundrecht auf freie Entfaltung der Persönlichkeit und drückt den Anspruch aller Menschen darauf aus, dass öffentliche und private Stellen in würdevoller und respektvoller Weise mit Informationen über sie umgehen. Nur die Betroffenen selbst sollen darüber entscheiden dürfen, wer ihre Daten erhält und wer nicht. Angesichts der besonderen Gefahren für das Persönlichkeitsrecht, die aus der rasanten technischen Entwicklung folgen, hat das Bundesverfassungsgericht in seinem Urteil zur Rechtswidrigkeit der Onlineüberwachung zusätzlich das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme entwickelt. Diese beiden Datenschutzgrundrechte gehören zum Menschenrechtsbollwerk in Zeiten der Wirtschaftskrise. Die Aufgabe, gemeinsam mit meinen Mitarbeiterinnen und Mitarbeitern mit dafür zu sorgen, dass diesen Menschenrechten in Bremen und Bremerhaven ein großes Gewicht beigemessen wird, empfinde ich als große Ehre.

Der Grad der Beachtung, den der Datenschutz als Ausformung des Menschenrechts auf informationelle Selbstbestimmung im Staat, in der Wirtschaft und in der Gesellschaft erfährt, ist Ausdruck der Beachtung der Menschenrechte allgemein. Angesichts der öffentlichen Diskussionen über die in den letzten Jahren laufend aufgedeckten Fälle der Missachtung dieser Rechte hat sich unser aller Bewusstsein über unsere Rechte im Zusammenhang mit dem Datenschutz schon deutlich geschärft. Aber wir müssen uns alle immer wieder neu darüber klar werden, wo die Grundrechte gefährdet und deshalb schutzbedürftig sind.

So ist das Bedürfnis, bestimmte Dinge nicht zu offenbaren, das ureigene Recht der Menschen, dessen Bedeutung wir alle selbst kennen. Das verkennt der neuerdings oft geäußerte Satz „Wer nichts zu verbergen hat, hat nichts zu befürchten." Im Gegenteil darf daraus, dass jemand dieses Recht auf das Verschweigen in Anspruch nimmt, nicht gefolgert werden, dass dieser Mensch etwas Unrechtes verbergen will. Völlig zu Recht steht deshalb beispielsweise auf den „gelben Zetteln", die Ärztinnen und Ärzte ausfüllen, um zu bestätigen, dass Menschen krankheitsbedingt nicht arbeiten können, ganz bewusst nicht die Diagnose. Zu wissen, dass und für wie lange die Menschen arbeitsunfähig sind, muss der Chefin oder dem Chef reichen. Um welche Krankheit es sich handelt, geht erst einmal niemanden etwas an.

**Datenschutz als Eindeichung der Menschenrechte gegen die Flut der Informationsbegehrlichkeiten**

Wir leben im Informationszeitalter, in dem Menschen mit Informationen überflutet werden. Der Dienstsitz der Bremischen Landesbeauftragten für Datenschutz und Informationsfreiheit liegt in Bremerhaven, nicht weit hinter dem Seedeich. Angesichts des Klimawandels werden den Bremerhavener Deichen in den nächsten Jahren viele Höhenzentimeter hinzugefügt. Auch die Deiche gegen die Flut der Informationsbegehrlichkeiten müssen dringend erhöht werden. Die Schlüsselqualifi-

kation in der Informations-, oder besser Wissensgesellschaft, die Fähigkeit, erkennen zu können, welche Informationen relevant sind und welche nicht, ist noch unterentwickelt. Als Beispiel hierfür kann die Kritik des US-amerikanischen Präsidenten Obama im Zusammenhang mit dem Anschlagsversuch zum Ende des Berichtsjahres dienen. Es hat sich herausgestellt, dass US-Behörden vom Vater des Betroffenen über dessen Attentatspläne informiert worden waren, dass diese Informationen aber nicht genutzt wurden, weil die entsprechenden Dateien riesige Mengen von Informationen aufwiesen und es an einer sinnvollen Auswertung fehlte. Der in Vorratsdatenspeicherungen zum Ausdruck kommenden Sammelwut staatlicher Institutionen ist ein „weniger ist mehr" entgegenzuhalten.

Angesichts der Sicherheitspanne im Januar 2010 auf dem Münchener Flughafen, bei der mutmaßlich schlecht bezahltes privates Sicherheitspersonal einen – wie sich herausstellte – fälschlich Verdächtigten nicht verfolgte, wurde die Forderung laut, es sei wichtiger, in die Menschen und ihre arbeitplatzbezogene Ausbildung zu investieren, als in immer neue Techniken, die wieder neue Datenfluten produzieren. Dieses Resümee „Kontrolle statt Scanner" (Frankfurter Rundschau vom 22. Januar 2010) sollten wir im Kopf behalten, wenn es demnächst um den Einsatz der sogenannten Körperscanner zur Flugsicherung geht. Wissensmanagement, die Fähigkeit, kompetent, effizient, verantwortungsbewusst und respektvoll mit Informationen über Menschen umzugehen, ist das Gebot der Stunde.

**Generalverdacht ersetzt die Unschuldsvermutung**

Das Bundesverfassungsgericht hat im Berichtsjahr über eine anlasslose sechsmonatige Speicherung aller Telekommunikationsverbindungsdaten (Wer telefoniert oder mailt mit wem zu welcher Zeit und wie lange und bei Mobiltelefonen auch noch von welchem Ort aus?) verhandelt. Dieses Beispiel für Vorratsdatenspeicherung zeigt, dass die im Anschluss an den 11. September 2001 verabschiedeten Antiterrorgesetze die Logik der rechtsstaatlichen Unschuldsvermutung umkehren. Alle Menschen müssen es sich gefallen lassen, ohne einen konkreten Anlass dafür geliefert zu haben, Maßnahmen ausgesetzt zu werden, die zuvor nur gegen Verdächtige möglich waren. Erst einmal stehen alle unter potenziellem Verdacht. Erst weitere Kontroll- oder Überwachungsmaßnahmen können ihre Entlastung ergeben. Die Grenzen zwischen Unschuldigen und Schuldigen, zwischen Unverdächtigen und Verdächtigen werden fließend. Diese Veränderung wird von vielen als Wandlung des Rechtsstaates in einen Präventionsstaat wahrgenommen, in dem alle Bürgerinnen und Bürger nicht mehr als unverdächtig, sondern als potenziell verdächtig, als „noch" nicht verdächtig betrachtet werden (Heribert Prantl). Die Freiheitsräume werden in einem solchen Staat immer kleiner. Hier ist zu hoffen, dass das Bundesverfassungsgericht in seinem für das Frühjahr 2010 angekündigten Urteil den beschriebenen Tendenzen Einhalt gebietet.

**Mangelnde Eignung zur Erreichung des verfolgten Zwecks**

Manchmal ist das Datensammeln zudem völlig ungeeignet zur Erreichung des verfolgten Zwecks. Großes Aufsehen erregte im Berichtsjahr die Diskussion über das SWIFT-Abkommen, das die EU mit den USA abschließen wollen. Dieses Abkommen soll es ermöglich, Bankdaten europäischer Bürgerinnen und Bürger an die USA weiterzugeben (vergleiche Ziffer 14.4 dieses Berichts). Dazu berichtete die Presse Anfang des Jahres 2010, dass das Bundeskriminalamt das von allen Datenschutzbeauftragten stark kritisierte Abkommen „für nutzlos beim Vorgehen gegen den internationalen Terrorismus" hält. Die aus fachlicher Sicht zu erwartenden Erkenntnisse rechtfertigten nicht den mit der Datenrecherche verbundenen erheblichen materiellen und personellen Aufwand. In diesem Zusammenhang ist wichtig, dass Maßnahmen rechtswidrig sind, die zur Erreichung eines vom Gesetzgeber festgelegten Zieles ungeeignet sind.

**Datenschutz als Instrument der Qualitätssicherung**

Datenschutz, der Schutz des Grundrechts auf informationelle Selbstbestimmung, kostet nicht unbedingt Geld, aber immer Gehirnschmalz. Die These aller Datenschützerinnen und Datenschützer ist, dass es in der Verwaltung wie in der Wirtschaft immer qualitätssteigernd wirkt, sich Gedanken darüber zu machen, wer wann welche Information benötigt und wie er oder sie diese rechtmäßig und mit dem geringsten Eingriff in Persönlichkeitsrechte erlangen kann. Gerade das Herausfinden, welche Informationen wann relevant sind, ist ein zugegebenermaßen aufwändiger Schritt, der in vielen Prozessen fehlt und sie zu lang und – das spielt in Bre-

men ja eine besonders wichtige Rolle – zu teuer macht. Auf diese Weise kann auch zu einem frühen Zeitpunkt identifiziert werden, welche Informationen zwar vielleicht wünschenswert wären, aber nicht auf gesetzlichem Wege erlangt werden können.

Für solche Qualitätssicherungsmaßnahmen im Zusammenhang mit der Modellierung von Arbeitsprozessen und auch für andere Aktionen zur Messung der Datenschutztemperatur bieten wir als auf diesem Gebiet Spezialisierte hiermit noch einmal ausdrücklich unsere Hilfe an, weil wir wie alle Menschen lieber im Vorfeld mitgestalten, als nachher zu kritisieren. Wie dieser Bericht bezeugt, haben wir im letzten Jahr in Verwaltung und Wirtschaft in der überwiegenden Zahl der Fälle erlebt, dass der Austausch über datenschutzrechtliche Fragen dazu geführt hat, dass Datenschutzverstöße verhindert, abgestellt oder zumindest gemildert wurden.

**„Stopp der Jugendgewalt“**

Am Tag vor meiner Wahl berichtete der „Weser-Kurier“, dass im Projekt „Stopp der Jugendgewalt“ das Thema Datenschutz „offenbar zu kurz gekommen“ sei. Das hat sich mittlerweile in den meisten der vielen Einzelprojekte geändert (vergleiche Ziffer 7.2 und Ziffer 5.2 dieses Berichts).

Die größte datenschutzrechtliche Herausforderung in dem Projekt ist der erklärte Wille, Informationen gleichzeitig an mehrere Stellen mit unterschiedlichen Aufgaben weiterzugeben. In solchen Konstellationen muss gewährleistet sein, dass nicht nach dem Motto „Jeder sagt allen alles, für irgendetwas wird es schon gut sein . . .“ ein der Vorratsdatenspeicherung strukturell gleichgelagerter Fall entsteht. So lange es zwei Akteure gibt, ist die Beurteilung einfach: Anknüpfungspunkt ist die Frage, wer welche Informationen zu welchem Zweck braucht. Handelt es sich um einen legitimen gesetzlichen Zweck und ist die Informationsweitergabe der einen an die andere Stelle gesetzlich vorgesehen und geeignet, den Zweck zu erreichen, so muss gefragt werden, ob es im Vergleich zur Informationsweitergabe nicht andere, ebenso geeignete Mittel gibt. Ist das nicht der Fall und steht die Informationsweitergabe auch nicht außer Verhältnis zu dem gesetzlichen Ziel, so ist sie rechtmäßig.

Komplizierter wird es dann, wenn eine Information – wie beispielsweise bei den geplanten Fallkonferenzen – durch eine Handlung (nämlich die Äußerung in einer Gruppe) gleich an mehrere Institutionen weitergegeben wird. Dann muss jede dieser Informationsweitergaben rechtmäßig sein. In den Fällen, in denen beispielsweise gesetzlich erlaubt oder sogar gefordert wird, dass eine Information vom Amt für Soziale Dienste an die Polizei gelangt, eine gesetzliche Übermittlungserlaubnis an die ebenfalls in der Konferenz sitzende Schule aber nicht existiert, wird es für diese zweite Informationsübermittlung schwierig. Hier fehlt es unter Umständen schon an der Eignung der Informationsübermittlung zur Erfüllung des gesetzlichen Ziels, das die Stelle verfolgt, die die Information nur deshalb mithört, weil sie mit am Tisch sitzt.

Als datenschutzrechtliche Lösung für die Fallkonferenzen diskutierten wir mit dem Senat über das Ob und das Wie von Einwilligungen der Betroffenen in Datenweitergaben.

**Privatisierungstendenzen im Zusammenhang mit der öffentlichen Sicherheit**

In der durch Medienberichte bestärkten öffentlichen Wahrnehmung ist die öffentliche Sicherheit zunehmend gefährdet. In einer Situation, in der die öffentliche Hand auch im Bereich der Polizei Personal tendenziell abbaut, öffnet sich damit eine Schere zwischen den ansteigenden Aufgaben und den tatsächlich zur Erfüllung dieser Aufgaben zur Verfügung stehenden Beschäftigten. Auf diese Situation wird zum Teil mit der Einbeziehung Privater in die Aufgabenerfüllung reagiert. Die Einbeziehung Privater findet ihre Grenze dort, wo der Bereich der Prävention, also der Verhinderung von Straftaten, verlassen wird und es um die Strafverfolgung bereits begangener Taten geht. Die Aufgaben der Strafverfolgung sind den hoheitlich tätigen und hierfür ausgebildeten Polizistinnen und Polizisten beziehungsweise der Staatsanwaltschaft vorbehalten.

Im Berichtsjahr gab es auch in Bremen Bestrebungen zur Privatisierung der Aufgabe der öffentlichen Sicherheit. Zwischen dem Senator für Inneres und Sport und dem Bundesverband Deutscher Wach- und Sicherheitsunternehmen e. V. (BDWS) wurde die „Vereinbarung zur Verbesserung der Sicherheit in Bremen“ abgeschlossen. Danach sollte eine neu einzurichtende gemeinsame Informations- und An-

sprechstelle der Mitglieder des BDWS der Polizei bedeutsame Informationen für „die Kriminalprävention, die Kriminalrepression und die Gefahrenabwehr“ mitteilen. Die Polizei sollte ein „gemeinsames Sicherheitslagebild“ erstellen und dies an die Sicherheitsunternehmen übermitteln. Der Senator für Inneres und Sport hat die Polizei gebeten, die beabsichtigte Kooperation „in dieser Form“ nicht weiter zu betreiben, woraufhin die Vereinbarung einvernehmlich wieder aufgehoben wurde.

Aus unserer Sicht gehört auch der Einsatz von Sprühanlagen mit „künstlicher DNA“ in diesen Zusammenhang (vergleiche Ziffer 5.1 dieses Berichts). Gegen den Diebstahlschutz durch die Markierung von Gegenständen mit der lackartigen Flüssigkeit haben wir keine grundsätzlichen Bedenken. In der Besprühung von Menschen mit „künstlicher DNA“ durch eine kurz zuvor von Privaten aktivierte Lichtschranke – und damit in der Markierung dieser Menschen als einer Straftat Verdächtige – sehen wir dagegen einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung, für den sich Private auf keine Rechtsgrundlage berufen können und der daher für Private nicht zu rechtfertigen ist. Da diese Markierung die spätere Strafverfolgung erleichtern soll, handelt es sich nach unserer Auffassung bei der Besprühung um eine Maßnahme der Strafverfolgung. Zur Strafverfolgung sind die hierfür ausgebildeten Polizistinnen und Polizisten zuständig. Für eine Markierung von Menschen durch Private zur Erleichterung der Strafverfolgung gibt es unseres Erachtens gegenwärtig keine Rechtsgrundlage. Unserer Auffassung nach ist der Grund hierfür unter anderem die zutreffende Einschätzung des Gesetzgebers, dass Private für Strafverfolgungsmaßnahmen nicht genügend ausgebildet sind. Im Gegensatz dazu erlernen Polizistinnen und Polizisten deeskalierende Techniken und können deshalb angemessen reagieren, wenn beispielsweise ein besprühter Waffenträger aus Wut über die von einem eindeutig identifizierbaren anderen Menschen ausgelöste Besprühung wieder zurückkehrt. In der vom Senat angekündigten polizeilichen Beaufsichtigung des privaten Einsatzes von „DNA-Sprühanlagen“ sehen wir deshalb einen Fortschritt für den Schutz des Grundrechts auf informationelle Selbstbestimmung. Gleichwohl vertreten wir die Auffassung, dass sich auch die so gestaltete Einbeziehung Privater nicht auf eine gesetzliche Grundlage berufen kann.

**Unterschiede bei der Kontrolltätigkeit über die Verwaltung und über Private**

Datenschutzrechtliche Regelungen wirken in der Verwaltung in folgender Weise: Aus dem Rechtsstaatsgebot folgt das Prinzip der Gesetzmäßigkeit der Verwaltung. Im öffentlichen Bereich gehört das Datenschutzrecht zu den Rechtsnormen, die die Verwaltung zu beachten hat. Wenn die Landesbeauftragte für Datenschutz und Informationsfreiheit und die Verwaltung gleichermaßen zu dem Ergebnis kommen, dass Verwaltungshandeln das Datenschutzrecht verletzt, wird dies abgestellt. Komplizierter wird es, wenn – wie dies gelegentlich der Fall ist – die Meinungen darüber auseinandergehen, ob ein Verwaltungshandeln wegen Verstoßes gegen datenschutzrechtliche Regelungen als rechtswidrig anzusehen ist oder nicht. Dann geht es um juristische Fragen, die ja bekanntermaßen von verschiedenen Juristinnen und Juristen unterschiedlich beantwortet werden können. Die Landesbeauftragte für Datenschutz und Informationsfreiheit vertritt dabei ihrem gesetzlichen Auftrag entsprechend im Zweifel die Auffassung, bei der das Grundrecht auf informationelle Selbstbestimmung am stärksten geschützt wird. Dass die Verwaltung das Grundrecht auf informationelle Selbstbestimmung besonders im Fokus hat, ist wichtig, weil sie eine Vorbildfunktion für die Wirtschaft hat, in der sich die Datenmissbrauchsskandale der letzten Jahre ja vor allem zugetragen haben.

Die Wirkungsweise von datenschutzrechtlichen Regelungen in der Wirtschaft ist eine andere. Dort gibt es zunehmend „Compliance“-Abteilungen, Regelungsüberwachungsabteilungen, die für das regelkonforme Verhalten eines Unternehmens im Hinblick auf alle gesetzlichen Ge- und Verbote sorgen sollen. Ziel der Compliance ist die Vermeidung von Kosten, insbesondere durch Schäden, Strafzahlungen, notwendige Maßnahmen oder Imageschäden. Der erste Arbeitsschritt ist deshalb die Identifikation und Analyse des „rechtlichen Risikos“. Hier ist es für die Durchsetzung datenschutzrechtlicher Standards ungünstig, wenn das Risiko, „erwischt“ zu werden, relativ gering ist, weil der Landesbeauftragten für Datenschutz und Informationsfreiheit aufgrund der Ressourcenknappheit zu wenige anlassunabhängige Kontrollen möglich sind. Ebenfalls ungünstig für die Durchsetzung datenschutzrechtlicher Standards ist es, wenn die durch Regelverletzungen entstehenden Kosten für die betreffenden Privaten nicht ins Gewicht fallen. Die im Zuge der Novellierung des Bundesdatenschutzgesetzes (vergleiche Ziffer 13.1 dieses Be-

richts) erfolgte Erhöhung des Bußgeldrahmens auf 300 000 Euro war hier ein Schritt in die richtige Richtung.

Für den Bereich der Datenschutzkontrolle über den öffentlichen Bereich sieht das Bremische Datenschutzgesetz eine Stellungnahme des Senats zum Jahresbericht der Landesbeauftragten für den Datenschutz vor, die im Parlament gemeinsam mit dem Jahresbericht beraten wird. Leider gibt es im Bundesdatenschutzgesetz keine entsprechende Regelung für eine Stellungnahme der Wirtschaft zu den im Bericht genannten Datenschutzverstößen im nicht öffentlichen Bereich.

**Internetsperren**

Nach heißer Diskussion wurde im Berichtsjahr das Gesetz über Internetsperren verabschiedet. Das Strafgesetzbuch gilt uneingeschränkt auch für Handlungen im Zusammenhang mit dem Internet. Es ist dort aufgrund der technischen Spezifika jedoch in der Regel schwerer durchzusetzen. Bei der Debatte um die Internetsperren ging es darum, was der Staat im Internet darf. Das Gesetz sah vor, dass die Internetnutzerinnen und Internetnutzer mit einem „Stoppschild" konfrontiert werden, wenn sie Seiten mit Inhalten öffnen wollen, auf denen Kindesmissbrauch gezeigt wird. Auch die Befürworterinnen und Befürworter der Internetsperren gingen davon aus, dass die Sperren relativ leicht zu umgehen sind und dass das einzig sichere Mittel, den Zugang zu diesen Seiten zu verhindern, die Löschung dieser Internetseiten ist. Daher war der eigentliche Gegenstand der Debatte der, ob der Staat die von allen Seiten nicht infrage gestellte gesellschaftliche Ächtung des Kindesmissbrauchs und des strafbaren Herunterladens der entsprechenden Internetseiten mit Hilfe der Internetsperren lediglich dokumentieren soll, obwohl es ein Mittel, die Löschung, gibt, das die Straftat des Herunterladens der Seiten sogar verhindern kann und, obwohl es ein durch die größte Massenpetition der Bundesrepublik – 135 000 Petentinnen und Petenten – dokumentiertes Misstrauen gegen den Staat gibt, dass er das einmal vorhandene Werkzeug der Internetsperren auch für die Sperrung von anderen Internetinhalten benutzt. Die Koalitionsvereinbarung auf Bundesebene sieht nun vor, dass das Gesetz ein Jahr lang nicht zur Anwendung kommt und stattdessen die Löschungsmöglichkeiten von Internetseiten mit rechtswidrigen Inhalten effektiviert werden. Die Ergebnisse dieser Bemühungen sollen evaluiert werden, bevor das Gesetz wieder zur Anwendung gelangen soll.

Diese Situation bietet die Möglichkeit, die gesellschaftliche Diskussion darüber zu führen, in welchem Grad Freiheit im Internet gewahrt werden muss und soll und an welchen Stellen – über die bereits bestehenden Regelungen hinaus – Regelungen getroffen werden müssen und sollen.

**Datenschutz als Bildungsaufgabe**

Die Bremische Bürgerschaft hat im Herbst 2008 in ihren Beschlüssen zum Datenschutz die Schaffung beziehungsweise Stärkung des Datenschutzbewusstseins der Bremerinnen und Bremer angemahnt. Menschenrechtsbildung, zu der auch das Wissen über das Grundrecht auf informationelle Selbstbestimmung und über das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme gehört, muss also auf die Tagesordnung gelangen. Wir, die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, haben dazu in unserer Herbstsitzung in Berlin gefordert, dass der Datenschutz zur Bildungsaufgabe wird (vergleiche Ziffer 16.11 dieses Berichts). Nach unserer Konzeption geht es dabei darum, die informationelle Selbstverantwortung aller Menschen, nicht nur der jungen, zu stärken. Dazu müssen die Grundrechte auf informationelle Selbstbestimmung und auf Vertraulichkeit und Integrität informationstechnischer Systeme zunächst inhaltlich vermittelt werden. Ihre Ableitung aus der Menschenwürde und dem Grundrecht auf freie Entfaltung der Persönlichkeit müssen ebenso wie ihre Bedeutung für die Einzelnen und die Gesellschaft deutlich werden. In einem zweiten Schritt müssen die Menschen von den diesen Rechten drohenden Gefahren erfahren. Sie müssen über die Gefahren im Internet, aber auch über die in der realen Welt aufgeklärt werden. Es soll allen Menschen bewusst werden, wo sie Datenspuren hinterlassen, wer diese lesen kann und welche Konsequenzen dies für die Einzelnen haben kann. Im dritten und wichtigsten Schritt muss den Menschen vermittelt werden, welche Möglichkeiten sie haben, um diesen Gefahren selbst begegnen zu können. Zum Selbstdatenschutz gibt es viele Vorschläge unter www.datenschutz.de, der Internetseite des Virtuellen Datenschutzbüros, des gemeinsamen Services der Datenschutzinstitutionen des Bundes und der Länder, sowie auf unserer Homepage unter www.datenschutz.bremen.de.

Die Bildungsaufgabe Datenschutz braucht allerdings nicht bei null anzufangen. Angesichts der öffentlich gewordenen Skandale im Umgang mit personenbezogenen Daten ist unser aller Datenschutzbewusstsein bereits angewachsen. Einer Studie zufolge haben sogar mehr Menschen Angst davor, dass ihre Daten missbraucht werden, als dass ihr Eigentum angetastet wird. Es ist wichtig, das Datenschutzbewusstsein weiter zu stärken und neues zu wecken.

Vor allem, soweit es um die Jugendlichen geht, sollte diese Bildungsaufgabe nicht mit dem erhobenen Zeigefinger erfüllt werden. Schon gar nicht sollte Menschen von der Nutzung des Internets abgeraten werden. Das würde der gesellschaftlichen Realität nicht gerecht. Jugendliche und Erwachsene sind in der Lage, auch im Internet selbstbewusste Entscheidungen zu treffen, wenn sie informiert sind und auch sonst gelernt haben, Gelesenes kritisch zu hinterfragen. Und Jugendliche können sich gegenseitig, aber auch uns Erwachsenen beim technischen Selbstdatenschutz meistens sehr viel beibringen.

Die Datenschutzbeauftragten sind nicht die einzigen, die sich mit dem Thema auseinandersetzen. Zur Medienkompetenz ist vom bremischen Rathaus ein runder Tisch angekündigt worden, der die vielen Akteurinnen und Akteure, die allein in Bremen an diesem Thema arbeiten, zusammenbringen will, um gemeinsame Initiativen zu planen und vor allem auch, um bei diesem so drängenden Thema Doppelarbeit zu vermeiden.

**Ist Privatheit unmodern geworden?**

Was alle dabei unbedingt erfahren müssen, ist, dass auch im Internet gelegentlich ohne ihren Willen über sie entschieden wird: Der Gründer des sozialen Netzwerkes „Facebook" – und damit jemand, der an den Nutzerdaten gut verdient – ist der Auffassung, die Privatsphäre – und er meint nicht seine eigene, sondern die der Nutzerinnen und Nutzer seines Netzwerkes – sei „nicht mehr zeitgemäß". Es habe ein entsprechender sozialer Wandel stattgefunden. Übrigens nutzte er diese Äußerung als Begründung dafür, dass die Daten Name, Profilbild, Geschlecht, Wohnort, Freundeliste, alle abonnierten Seiten und so weiter der Nutzerinnen und Nutzer des von ihm kreierten sozialen Netzwerkes in der Grundeinstellung öffentlich sichtbar, und damit recherchierbar sind, und die Nutzerinnen und Nutzer diese Grundeinstellung jetzt aktiv verändern müssen, um ihre Daten nur denjenigen zur Verfügung zu stellen, denen sie sie offenbaren wollen.

Auch ein Zukunftskongress in Oldenburg prognostizierte im Berichtsjahr, dass die Menschen in zehn Jahren keine Wertschätzung mehr für die Privatheit haben würden. Dass die Nutzerinnen und Nutzer eines sozialen Netzwerkes ihre Privatsphäre nicht mehr für schützenswert halten, ist eine unbewiesene Behauptung, und darüber, ob die Menschen in zehn Jahren keine Wertschätzung mehr für ihr Recht auf Privatheit aufbringen werden, müssen sie schon selbst entscheiden! Jedenfalls wird niemand dieses Recht deshalb aufgeben wollen, weil er anderen die Möglichkeit geben will, an den dadurch gewonnenen Informationen zu verdienen.

Wir alle können an uns bemerken, dass das Gefühl, beobachtet zu werden, das Verhalten verändert. Jedes Verhalten, das wir unter diesem Gefühl an den Tag legen, bezieht sich auf den Umstand der Beobachtung: Wenn ich im bekanntermaßen videoüberwachten, ansonsten menschenleeren Raum bin, unterlasse ich es, in der Nase zu bohren, oder mache es trotzdem oder gerade aufgrund der Überwachung. Alle Handlungsweisen reflektieren jedenfalls die Situation, beobachtet zu sein. Dieses ständige Mit-Bewusstsein, in immer mehr sozialen Räumen nicht ohne potenzielles, aber nicht selbst sichtbares Gegenüber zu sein, sich der Beobachtung immer weniger entziehen zu können, verändert unseren Raum der Freiheit. Das Recht auf Privatheit wird immer mehr zum Luxus. Und das sollten wir nicht ohne eine große gesellschaftliche Debatte geschehen lassen. Und darin können wir dann auch daran erinnern, dass die Moderne einmal mit der Erklärung der Menschen- und Bürgerrechte zusammenhing.

**„Cookies löschen?"**

Auf der Titelseite dieses Berichts kommt das Krümelmonster in arge Bedrängnis: Kann es wirklich richtig sein, Cookies zu löschen? Was ist denn gegen Kekse einzuwenden? Cookies (Keks heißt auf Englisch Cookie) sind kleine Datenmengen, die zusammen mit den eigentlich angeforderten Daten aus dem Internet an den Computer übermittelt, dort gespeichert und für einen späteren Abruf der den Cookie sendenden Stelle bereitgehalten werden. Betreiber von Internetdiensten können

aus geeignet gewählten und eingerichteten Cookies ein Nutzungsprofil erstellen, das vielfältige Auskunft über die Nutzerin oder den Nutzer gibt. Eine Manipulation des Computers über Cookies selbst ist nicht möglich. Allerdings können Unberechtigte mit anderen Mitteln auf die Datei auf dem Computer zugreifen, in der die Cookie-Informationen, die auch benutzerbezogene Passwörter für Internetseiten, zum Beispiel von Banken, umfassen können, gespeichert werden. Das Hauptproblem an Cookies ist ihre mangelnde Transparenz: Der Datenaustausch mittels Cookies erfolgt zwischen den beteiligten Computern vollkommen im Hintergrund, ohne dass die Nutzerinnen und Nutzer über Inhalte, Zweck, Umfang, Speicherdauer oder Zugriffsmöglichkeiten auf die Cookie-Daten informiert werden, sofern sie keine besonderen Maßnahmen ergreifen. Diese Parameter sind innerhalb der Cookies selbst festgelegt und werden damit allein vom Betreiber des Internetservers bestimmt. Es hängt von der Initiative der Nutzerinnen und Nutzer ab, ob sie sich vor Cookies schützen können oder diese zumindest bemerken und dann löschen können.

Was können Sie also tun? Sie können Ihren Browser so konfigurieren, dass Cookies nicht oder wenigstens nicht automatisch akzeptiert und Cookies, die gespeichert werden sollen, angezeigt werden. Bereits gespeicherte Cookies können gelöscht werden, zum Beispiel die Datei cookies.txt bei Netscape-Browsern. Außerdem können Sie Cookie-Filter einsetzen. Und wenn Sie das alles geschafft haben, dann können Sie sich in Ruhe genüsslich einen Keks gönnen. Aber bitte nicht so krümeln . . .

Dr. Imke Sommer

Die Landesbeauftragte für Datenschutz
und Informationsfreiheit der Freien Hansestadt Bremen

## 2. Bremische Bürgerschaft

### 2.1 Ergebnisse der Beratungen des 31. Jahresberichts

Bericht und Antrag des Ausschusses für Informations- und Kommunikationstechnologie und Medienangelegenheiten (Medienausschuss) zum 31. Jahresbericht des Landesbeauftragten für Datenschutz vom 27. Februar 2009 (Drucksache 17/706) und zur Stellungnahme des Senats vom 25. August 2009 (Drucksache 17/903)

**I. Bericht**

Die Bürgerschaft (Landtag) überwies in ihrer Sitzung am 18. März 2009 den 31. Jahresbericht des Landesbeauftragten für den Datenschutz vom 27. Februar 2009 (Drucksache 17/706) und in ihrer Sitzung am 1. Oktober 2009 die dazu erfolgte Stellungnahme des Senats vom 25. August 2009 (Drucksache 17/903) an den Ausschuss für Informations- und Kommunikationstechnologie und Medienangelegenheiten zur Beratung und Berichterstattung.

Der Ausschuss beschäftigte sich in seinen Sitzungen am 19. Juni und 30. Oktober 2009 mit dem 31. Jahresbericht sowie der Stellungnahme des Senats und stellte bei den nachfolgend aufgeführten Punkten Beratungsbedarf fest:

1. Ziffer 6.4 Administrativer Zugang am Dataport-Standort Bremen
2. Ziffer 9.2 Übermittlung von Meldedaten an Adresshändler
3. Ziffer 9.4 Entwurf eines Bundesmeldegesetzes
4. Ziffer 9.5 Überwachung auf der „Discomeile“
5. Ziffer 9.6 Aktualisierte KpS-Richtlinien
6. Ziffer 10.2 Soziale Dienste bei der Justiz

In seiner Sitzung am 30. Oktober 2009 erörterte der Ausschuss die beratungsbedürftigen Punkte mit der Landesbeauftragten für den Datenschutz unter Hinzuziehung von Vertreterinnen und Vertretern der betroffenen Ressorts.

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

1. Administrativer Zugang am Dataport-Standort Bremen (Ziffer 6.4): Der Ausschuss nimmt zur Kenntnis, dass der administrative Zugang am Dataport-Standort Bremen noch nicht frei geschaltet worden ist. Derzeit wird daran gearbeitet, den Zugang zu Dataport so zu gestalten, dass die Sicherheitsanforderungen erfüllt sind. In dieser Hinsicht besteht sowohl nach Auffassung der Senatorin für Finanzen als auch der Landesbeauftragten für den Datenschutz noch Verbesserungsbedarf. Der Ausschuss weist nachdrücklich darauf hin, dass die datenschutzrechtlichen Belange unbedingt eingehalten werden müssen und die Schaffung einer konsolidierten Architektur von Datenport nicht zu Lasten des Datenschutzes gehen darf.

2. Übermittlung von Meldedaten an Adresshändler und Entwurf eines Bundesmeldegesetzes (Ziffer 9.2 und Ziffer 9.4): Nach den melderechtlichen Bestimmungen dürfen die Meldebehörden im Land Bremen Auskünfte über im Melderegister gespeicherte Personen auch an Privatpersonen erteilen. Bei dieser sogenannten einfachen Melderegisterauskunft wird Auskunft über den Vor- und Familiennamen, den Doktorgrad sowie die aktuelle Anschrift gegeben. Diese Auskunft ist nicht mit Auflagen verbunden, das heißt die antragstellende Person muss weder den Grund angeben, wofür die Daten benötigt werden noch wird sie verpflichtet, die Daten nach einer bestimmten Zeitspanne wieder zu löschen. Einzige Voraussetzung für die Auskunftserteilung ist, dass die auskunftsersuchende Person oder Stelle den Betroffenen beziehungsweise die Betroffene hinreichend bestimmt. Die Problematik der einfachen Melderegisterauskunft besteht darin, dass im Rahmen dieses Verfahrens teilweise auch Daten an Adresshändler weitergegeben werden, die im Auftrag eines Unternehmens oder einer Privatperson als Adressermittler tätig werden. Diese Adresshändler beschränken sich in der Regel nicht darauf, die Daten weiterzugeben, sondern bauen eigene private Melderegister („Schattenregister“) auf. Dieses Vorgehen ist sowohl mit datenschutzrechtlichen Anforderungen als auch mit den Vorgaben des Melderechts nicht zu vereinbaren. Vor dem Hintergrund der zahlreichen Datenskandale im letzten Jahr und in den vergangenen Monaten

erachtet es der Ausschuss für wichtig, dass dieser zweckwidrigen Verwendung von Daten wirksam begegnet wird und die schutzwürdigen Interessen der Betroffenen stärker berücksichtigt werden. Im Hinblick auf die geltenden Rechtslage, die der Meldebehörde auch bei der einfachen Melderegisterauskunft ein Ermessen bei der Auskunftserteilung einräumt, ist nach Auffassung des Ausschusses zu überlegen, ob dieses Instrument nicht genutzt werden kann, um die Weitergabe von Daten an Adresshändler künftig zu verhindern oder zumindest einzuschränken. Dabei sollte auch darüber nachgedacht werden, dieses Problem im Land Bremen nach dem Vorbild anderer Bundesländer im Wege eines entsprechenden Erlasses zu regeln. Mit dem Gesetz zur Änderung des Grundgesetzes vom 28. August 2006 wurde dem Bund die ausschließliche Gesetzgebungskompetenz für das Melde- und Ausweiswesen übertragen. Der erste Entwurf eines Bundesmeldegesetzes liegt bereits vor. Derzeit ist jedoch noch nicht absehbar, wann dieses in Kraft treten wird und in welcher Form es sich dem oben geschilderten Problem mit dem Adresshandel annehmen und dieses lösen wird. Deshalb sollte nach Ansicht des Ausschusses nicht abgewartet werden, bis das Bundesmeldegesetz in Kraft tritt, sondern zeitnah eine bremische Lösung des Problems gefunden werden. Der Ausschuss wird sich mit dieser Thematik weiterhin befassen und sich vom Innenressort über die aktuellen Entwicklungen unterrichten lassen.

3. Videoüberwachung auf der Discomeile (Ziffer 9.5): Die im Bericht bemängelte nicht hinreichende Beschilderung des kameraüberwachten Bereiches auf der Discomeile wurde nach Auskunft der Ressortvertreterin inzwischen behoben und ein zusätzliches Schild im betroffenen Bereich angebracht. Ein offenes datenschutzrechtliches Problem ist nach wie vor die private Videoüberwachung der Notausgänge einer Diskothek, die in ein privates Treppenhaus führen. Die Mieterinnen und Mietern des Gebäudes werden durch die installierten Kameras gegen ihren Willen mit überwacht. Zur Lösung des Problems wurde nunmehr ein Termin zur Ortsbesichtigung vereinbart, an dem unter anderen auch Vertreterinnen und Vertreter der Polizei, des Innenressorts sowie die Landesbeauftragte für den Datenschutz teilnehmen werden. Der Ausschuss geht davon aus, dass alle Beteiligten eine einvernehmliche Lösung des Problems finden werden und erwartet, dass der Ausschuss zu gegebener Zeit über das Ergebnis informiert wird.

4. Aktualisierte KpS-Richtlinien (Ziffer 9.6): Die Richtlinien für die Führung Kriminalpolizeilicher Sammlungen (KpS-Richtlinien) legen allgemein für typische Sachverhalte der polizeilichen Arbeit fest, welche personenbezogenen Daten erhoben und gespeichert werden dürfen. Die personenbezogenen Hinweise (PHW) dienen vor allem der Eigensicherung der Polizei und werden im Rahmen der Einsatztaktik der Polizei berücksichtigt. In der Vergangenheit wurde im Rahmen der PHW bereits im Vorfeld der Feststellung einer psychischen Erkrankung das Merkmal „psychisch auffällig“ vergeben. Es bedurfte keiner Feststellung einer psychischen Erkrankung durch einen Arzt, sodass im Einzelfall die Vergabe des PHW „psychisch krank“ nicht genau verifizierbar war. Aufgrund von entsprechenden Beschwerden von Betroffenen und nach Hinweis der Landesbeauftragten für den Datenschutz auf die bestehende Problematik werden nunmehr nach Auskunft des Ressortvertreters bei der Polizei keine PHW „psychisch auffällig“ mehr vergeben. Künftig wird nur noch nach ärztlicher Feststellung der PHW „psychisch krank“ verwendet. Ein Problem bereitet derzeit nur noch der Umgang mit den sogenannten „Altfällen“, bei denen der PHW „psychisch auffällig“ bereits gespeichert ist. Der Aufgabe, hier eine Lösung zu erarbeiten, hat sich eine Arbeitsgruppe unter Beteiligung der Ressorts Gesundheit, Justiz und Inneres angenommen. Es ist vorgesehen, dass am Ende der Beratungen der Arbeitsgruppe eine Abstimmung der Ergebnisse mit der Landesbeauftragten für den Datenschutz erfolgt. Der Ausschuss begrüßt es, dass von einer Speicherung des PHW „psychisch auffällig“ nunmehr ganz abgesehen wird und sich die datenschutzrechtliche Problematik insofern erledigt hat. Er fordert aber nachdrücklich, dass die Landesbeauftragte für den Datenschutz bereits jetzt in die Arbeitsgruppe der Ressorts Gesundheit, Justiz und Inneres aufgenommen wird, da datenschutzrechtliche Aspekte in diesem Zusammenhang eine wichtige Rolle spielen.

5. Soziale Dienste bei der Justiz (Ziffer 10.2): Bei den Bewährungshelferinnen und Bewährungshelfern bestand und besteht zum Teil immer noch erhebliche Ver-

unsicherung darüber, ob und in welchem Umfang sie Informationen über ihre Klienten an Dritte übermitteln dürfen. Während die Weitergabe von Daten an das Gericht ausdrücklich gesetzlich geregelt ist, stellt sich bei Anfrage von anderen Behörden, insbesondere von Polizei und Staatsanwaltschaft, die Frage, ob die Bewährungshelferinnen und Bewährungshelfer zur Auskunftserteilung überhaupt befugt sind. Dies hängt im Wesentlichen davon ab, ob sie als Berufsgeheimnisträger einer besonderen Schweigepflicht gemäß § 203 Absatz 1 Nummer 5 Strafgesetzbuch (StGB) oder lediglich der allgemeinen Schweigepflicht gemäß § 203 Absatz 2 Seite 1 StGB unterliegen. In der Eigenschaft als Berufsgeheimnisträger würde eine unbefugte Weitergabe von Daten an Dritte eine Strafbarkeit nach dem Strafgesetzbuch begründen. In dieser Frage werden von Seiten des Justizressorts und der Landesbeauftragten für den Datenschutz unterschiedliche Rechtsauffassungen vertreten. Eine abschließende Klärung konnte bisher nicht herbeigeführt werden. Der Ausschuss nimmt zur Kenntnis, dass der Senator für Justiz zu dieser Problematik gegenüber den Bewährungshelfern und Bewährungshelferinnen eine Stellungnahme abgegeben hat, aus der eine Handlungsanweisung für die Praxis entwickelt worden ist. Er sieht aber dennoch weiteren Erörterungsbedarf, damit eine einvernehmliche Lösung gefunden wird, die den Bewährungshelfern und -helferinnen in ihrer praktischen Arbeit die größtmögliche Rechtssicherheit bietet. In diesem Zusammenhang begrüßt der Ausschuss den Beschluss der Justizministerkonferenz vom 5. November 2009 zu prüfen, ob in diesem Bereich die Schaffung ergänzender gesetzlicher Regelungen für den Austausch von personenbezogenen Daten sinnvoll ist. Der Ausschuss wird sich mit dieser Thematik weiter befassen und sich von den beteiligten Ressorts über die aktuellen Entwicklungen unterrichten lassen.

**II. Antrag**

Die Bürgerschaft (Landtag) möge beschließen:

Die Bürgerschaft (Landtag) tritt den Bemerkungen des Ausschusses für Informations- und Kommunikationstechnologie und Medienangelegenheiten bei.

## 3. Behördliche Beauftragte für den Datenschutz

### 3.1 Workshops der behördlichen Datenschutzbeauftragten 2009

Die Workshops mit den behördlichen Datenschutzbeauftragten der bremischen Verwaltung wurden im Frühjahr und Herbst 2009 fortgesetzt. Ressortübergreifend wurden in den Workshops schwerpunktmäßig erneut Themenbereiche behandelt, die an die personenbezogene Datenverarbeitung der Dienststellen besondere Anforderungen stellen und an deren Einhaltung die einzelnen behördlichen Datenschutzbeauftragten maßgeblich beteiligt sind. Ziel der Workshops ist es jeweils, die Datenschutzbeauftragten bei der Wahrnehmung ihres schwierigen Amtes möglichst praxisorientiert zu unterstützen.

Der im Frühjahr 2009 durchgeführte Workshop befasste sich schwerpunktmäßig mit dem Thema Personaldatenschutz. Die ordnungsgemäße Verarbeitung von Personaldaten ist auch in der öffentlichen Verwaltung ein äußerst brisantes Thema, das für die Erfüllung der Aufgaben der behördlichen Datenschutzbeauftragten in ihren Dienststellen von hoher Bedeutung ist. Nicht zuletzt wegen der in der Privatwirtschaft bei der Verarbeitung von Arbeitnehmerdaten festgestellten schwerwiegenden Mängel haben sich auch in den Behörden verstärkt Fragen zur Verarbeitung von Personaldaten ergeben, zu deren Lösung die behördlichen Datenschutzbeauftragten in erheblichem Umfang beitragen müssen. Neben den allgemeinen Regelungen zur Personaldatenverarbeitung wurden im Workshop speziell Fragen zur Verarbeitung von Personaldaten in den Bereichen der Telekommunikation, der Telearbeit, des Betrieblichen Eingliederungsmanagements und der Korruptionsbekämpfung angesprochen. Neben einem Fachreferat zum Thema durch den für Personal- und Arbeitnehmerdatenschutz zuständigen Referatsleiter der Landesbeauftragten für Datenschutz und Informationsfreiheit bestand für die Teilnehmerinnen und Teilnehmer des Workshops die Möglichkeit, ausführlich hierzu Fragen zu stellen, wovon rege Gebrauch gemacht wurde.

Der Workshop im Herbst 2009 befasste sich schwerpunktmäßig mit dem Thema Datenverarbeitung im Auftrag. Bei der Erteilung von Aufträgen, die die Verarbeitung personenbezogener Daten vorsehen, sind von den Dienststellen nach dem Bre-

mischen Datenschutzgesetz (BremDSG) zahlreiche gesetzliche Regelungen zu beachten. Hierdurch ergeben sich häufig Fragen, die zur Beantwortung den behördlichen Datenschutzbeauftragten vorgelegt werden. Auch die Landesbeauftragte für Datenschutz und Informationsfreiheit war 2009 verstärkt mit dem Thema befasst, zum Beispiel im Hinblick auf die Vergabe von Datenverarbeitungsaufträgen an Dataport (vergleiche Ziffer 4.2 dieses Berichts). Angesprochen wurden in dem Workshop insbesondere die Ziele und das Wesen der Regelungen zur Auftragsdatenverarbeitung und deren Folgen, die Abgrenzung von anderen Formen der Zusammenarbeit mit anderen Stellen, die Grenzen der Auftragsdatenverarbeitung, die Pflichten der Beteiligten, die bei der Auftragserteilung zu beachtenden Kriterien sowie die Mitwirkung der behördlichen Datenschutzbeauftragten bei der Vergabe und Durchführung von Datenverarbeitungsaufträgen. Im Workshop wurden auch die mit der Novellierung des Bundesdatenschutzgesetzes (BDSG) in § 11 dieses Gesetzes neu aufgenommenen Regelungen zur Datenverarbeitung im Auftrag dargestellt, die für den nicht öffentlichen Bereich insbesondere zu einer Konkretisierung hinsichtlich der einzuhaltenden Anforderungen an die Auftragsmindestinhalte und den Umfang der Kontrollverpflichtung und der Dokumentationspflicht geführt hat, was auch für den öffentlichen Bereich durch eine entsprechende Änderung des § 9 BremDSG wünschenswert wäre. Neben dem Referat durch den zuständigen Referatsleiter der Landesbeauftragten für Datenschutz und Informationsfreiheit wurden auch in diesem Workshop von den Teilnehmerinnen und Teilnehmern zum Thema zahlreiche Fragen gestellt und ausführliche Diskussionen geführt.

Aufgrund des großen Interesses der behördlichen Datenschutzbeauftragten an den Workshops wurden sowohl im Frühjahr als auch im Herbst 2009 jeweils zwei Veranstaltungen des Workshops mit gleichem Ablauf durchgeführt, sodass sich die Workshopteilnehmerinnen und -teilnehmer in zwei Gruppen aufgeteilt haben. Besonderer Dank für die Unterstützung bei der Durchführung der Workshops gilt dem Ortsamt Mitte / Östliche Vorstadt in Bremen, das den Veranstaltungsraum zur Verfügung stellte.

Erstmalig wurden im Jahr 2009 auch mit den behördlichen Datenschutzbeauftragten des Magistrats der Stadt Bremerhaven Workshops durchgeführt. Auch dort stießen die Veranstaltungen auf großes Interesse. Schwerpunktmäßig wurden im April und September 2009 die Themen Datenschutzmanagement bei den Ämtern und Betrieben des Magistrats und Personaldaten behandelt, wobei inhaltlich an die im Herbst 2008 beziehungsweise Frühjahr 2009 in Bremen vorangegangenen Workshops angeknüpft wurde. Spezielle Probleme und Fragestellungen in der Bremerhavener Stadtverwaltung sind jedoch nicht unberücksichtigt geblieben. Auch in diesen Workshops bestand ausführlich Gelegenheit, Fragen zu stellen und Probleme zu diskutieren, wovon reger Gebrauch gemacht wurde.

Die Teilnehmerinnen und Teilnehmer der Bremerhavener Workshops wiesen auch auf Probleme hin, die bei den Ämtern des Magistrats im Hinblick auf die Akzeptanz und das Verständnis des Amtes des behördlichen Datenschutzbeauftragten bestehen. Wir halten es für unerlässlich, dass die Amtsleitungen die uneingeschränkte Wahrnehmung der den behördlichen Datenschutzbeauftragten nach dem Bremischen Datenschutzgesetz zugewiesenen gesetzlichen Aufgaben sicherstellen.

Es ist beabsichtigt, die Reihe der Workshops in Bremen und Bremerhaven im Jahr 2010 fortzusetzen. Dabei soll der praktische Nutzen, den die Teilnehmerinnen und Teilnehmer aus den Veranstaltungen ziehen können, weiter verstärkt und noch mehr Gelegenheit zum gegenseitigen Erfahrungsaustausch gegeben werden.

### 3.2 Behördlicher Datenschutz im Bereich der Gesundheit Nord gGmbH

Die Gesundheit Nord gGmbH (GeNo) informierte uns im Juni 2009 über ihre Planungen, im Zuge der vorgesehenen Zentralisierungen der patientenfernen Verwaltungsbereiche der zum Klinikverbund gehörenden Kliniken Bremen-Mitte, Bremen-Ost, Bremen-Nord und Links der Weser (vergleiche Ziffer 7.7 dieses Berichts) einen zentralen Konzernbereich „Datenschutz“ einzurichten. Dieser Bereich soll an die den Verbund leitende GeNo angebunden werden. Sein Zuständigkeitsbereich soll alle datenschutzrechtlichen Angelegenheiten der zum Verbund gehörenden Stellen umfassen und verbundweit gültige Standardregelungen mit dem Ziel eines einheitlichen Datenschutzniveaus formulieren. Als Leiterin oder Leiter des Konzernbereichs Datenschutz soll von den zum Verbund gehörenden Stellen jeweils eine gemeinsame hauptamtliche Konzerndatenschutzbeauftragte oder ein

gemeinsamer hauptamtlicher Konzerndatenschutzbeauftragter bestellt, die bisherigen Datenschutzbeauftragten zuvor abberufen werden.

Die Planungen der GeNo stießen bei uns auf erhebliche datenschutzrechtliche Bedenken, da sie in mehreren Punkten nicht mit den Vorschriften der zu beachtenden Gesetze zu vereinbaren waren. Maßgeblich für die Bestellung, die Tätigkeit und die Abberufung von Datenschutzbeauftragten bei der GeNo ist § 7 a Bremisches Datenschutzgesetz (BremDSG) bei den vier zum Verbund gehörenden Kliniken in öffentlicher Trägerschaft ist es § 9 des Bremischen Krankenhausdatenschutzgesetzes (BremKHDSG) in Verbindung mit § 7 a Absätze 2 bis 5 BremDSG.

In unserer Stellungnahme gegenüber der GeNo wiesen wir insbesondere darauf hin, dass nach den zu beachtenden Vorschriften die Kliniken und die GeNo jeweils selbstständig und eigenverantwortlich eine Datenschutzbeauftragte beziehungsweise einen Datenschutzbeauftragten zu bestellen haben. Auch enge wirtschaftlich begründete und organisatorisch abgesicherte Beziehungsgeflechte vermögen nach den Datenschutzgesetzen nichts an der rechtlichen Selbstständigkeit der einzelnen personenbezogene Daten verarbeitenden Stellen zu ändern. Es wäre mit den datenschutzrechtlichen Vorgaben nicht zu vereinbaren, wenn die zum Verbund gehörenden Kliniken Datenschutzbeauftragte nach Vorgabe der GeNo bestellen würden.

Die Datenschutzbeauftragten haben die Stelle, von der sie bestellt worden sind, zu beraten und dort die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden, zu kontrollieren. Um ihre Aufgaben wahrnehmen zu können, müssen die Datenschutzbeauftragten mit den besonderen, für den jeweiligen Handlungskontext der Stelle, von der sie bestellt worden sind, relevanten Regelungen sowie den technischen und organisatorischen Gegebenheiten vertraut sein. Auch müssen sie über die notwendige Zuverlässigkeit verfügen. Die Zuverlässigkeit besteht unter anderem dann nicht, wenn die Tätigkeit der oder des Datenschutzbeauftragten zu einer Interessenkollision mit der Übertragung dieser Funktion auch bei einer anderen Stelle führt. Eine effektive Aufgabenerfüllung ist dann nicht mehr möglich. Erhebliche Bedenken im Hinblick auf die Vereinbarkeit der Aufgabenübertragung ergeben sich zum Beispiel bei Konzerndatenschutzbeauftragten, die sowohl von der den Konzernverbund leitenden Stelle als auch von einer oder mehreren anderen zum Verbund gehörenden Stellen zur beziehungsweise zum Datenschutzbeauftragten bestellt worden sind. Der spezifische Verantwortungsbereich der beziehungsweise des jeweiligen Beauftragten darf wegen der Selbstständigkeit und Eigenverantwortlichkeit der einzelnen zum Klinikverbund gehörenden Stellen nicht verletzt werden.

Nach den uns vorgelegten Planungen der GeNo sollte die oder der vorgesehene Konzerndatenschutzbeauftragte einerseits bei allen Stellen des Klinikverbundes die datenschutzrechtlichen Ziele der den Verbund leitenden Stelle kommunizieren, entsprechende Ablauforganisationen und einheitliche Datenschutzstandards zentral vorgeben, andererseits die Handlungen der einzelnen Stellen entsprechend der konkreten Gegebenheiten auf ihre Vereinbarkeit mit den einzuhaltenden datenschutzrechtlichen Anforderungen überprüfen müssen. Die Gewährleistung der Einhaltung der datenschutzrechtlichen Anforderungen ist nach dem BremDSG Aufgabe der jeweils verantwortlichen Stelle, hier also der GeNo und den einzelnen zum Verbund gehörenden Kliniken. Um diese Aufgabe wahrnehmen zu können, muss die verantwortliche Stelle insoweit selbst handlungs- und entscheidungsbefugt sein. Die auf eine Zentralisierung ausgerichtete Konzeption der GeNo läuft diesem Anspruch zuwider.

Eine besondere Unvereinbarkeit hinsichtlich der Übertragung der Funktion der beziehungsweise des behördlichen Datenschutzbeauftragten ergibt sich darüber hinaus, wenn die oder der Datenschutzbeauftragte bei einer Auftragsdatenverarbeitung gleichzeitig vom Auftraggeber und Auftragnehmer in dieses Amt bestellt worden ist. Der Auftraggeber und der Auftragnehmer haben bei einer Auftragsdatenverarbeitung unterschiedliche voneinander getrennte Rechte und Pflichten, deren Wahrnehmung nicht von der gleichen Person als Datenschutzbeauftragter oder Datenschutzbeauftragtem überwacht werden darf. Bei der Auslagerung personenbezogener Datenverarbeitung von den Kliniken zur GeNo im Rahmen einer Auftragsdatenverarbeitung würde sich bei einer Realisierung der von der GeNo dargelegten Planungen zur Bestellung einer oder eines Konzerndatenschutzbeauftragten auch hieraus eine Unvereinbarkeit ergeben.

Weitere erhebliche Bedenken ergeben sich hinsichtlich der Einhaltung der Bestimmungen des § 7 a BremDSG. Danach ist die oder der behördliche Datenschutzbeauftragte bei der Erfüllung ihrer oder seiner Aufgaben der Leitung der öffentlichen Stelle, die sie oder ihn bestellt hat, unmittelbar zu unterstellen. Sie oder er ist bei der Erfüllung ihrer oder seiner Aufgaben weisungsfrei und darf deswegen nicht benachteiligt werden. Die oder der behördliche Datenschutzbeauftragte darf deshalb auch nur gegenüber der Stelle, die sie oder ihn bestellt hat, nicht aber gegenüber einer anderen Stelle, wie in diesem Fall der den Verbund leitenden Stelle, rechenschaftspflichtig sein. Eingriffe in die Weisungsfreiheit, wie sie sich aus der Konzeption der GeNo insbesondere durch ihr Einwirken auf die Aufgabenwahrnehmung der oder des Konzerndatenschutzbeauftragten ergäben, wären nicht zulässig.

Schließlich kann die Bestellung der oder des Datenschutzbeauftragten nur bei entsprechender Anwendung von § 626 Bürgerliches Gesetzbuch (BGB), das heißt, aus wichtigem Grund, widerrufen werden. Ein wichtiger Grund, der bei den von dem zum Verbund gehörenden Stellen bislang bestellten Datenschutzbeauftragten eine Abberufung rechtfertigen würde, bestand nach unseren Erkenntnissen nicht.

Die GeNo teilte daraufhin in einem gemeinsamen Gespräch zu unserer Stellungnahme mit, dass sie auf die Einrichtung eines Konzernbereichs „Datenschutz“ und die Bestellung einer oder eines Konzerndatenschutzbeauftragten verzichten wolle. Sie schloss sich unserer Auffassung an, dass eine oder ein von der den Klinikverbund leitenden Stelle bestellte Datenschutzbeauftragte oder bestellter Datenschutzbeauftragter diese Funktion gleichzeitig nicht auch von einer oder mehreren Kliniken des Verbundes übertragen werden darf. Der bislang zugleich von ihr und dem Klinikum Bremen-Mitte bestellte Datenschutzbeauftragte soll daher mit diesem Amt bei der GeNo nicht länger betraut werden.

In einer uns erst nach dem Gespräch übersandten schriftlichen Stellungnahme wich die GeNo bedauerlicherweise in gravierendem Umfang von den von ihr zuvor getätigten Aussagen ab. Sie teilte uns mit, dass aus ihrer Sicht keine konfligierenden Interessen erkennbar seien, durch die die Bestellung einer oder eines gemeinsamen Datenschutzbeauftragten von den zum Klinikverbund gehörenden Stellen unzulässig erscheine. GeNo plane für den Verbund nicht, die Bestellung von Datenschutzbeauftragten verpflichtend zwischen ihr und den Kliniken zu trennen. Davon ausgehend, dass grundsätzlich nichts dagegen spricht, wenn sie für die anderen zum Klinikverbund gehörenden Stellen als Auftragnehmerin fungiert, was so allerdings nicht richtig ist, begründete die GeNo ihre Auffassung damit, dass sich bei der Auftragsdatenverarbeitung für die Gesellschaften des Klinikverbundes eine gänzlich andere Konstellation als bei sich fremden Vertragspartnern ergibt. Es beständen keine gegenläufigen wirtschaftlichen Interessen, die eine klare Trennung der Verantwortlichkeiten von Auftraggebern und Auftragnehmern erforderlich machen würden. Obgleich bei der gemeinsamen Bestellung einer oder eines gemeinsamen Datenschutzbeauftragten durch mehrere Stellen eines Konzernverbundes Bedenken hinsichtlich der Zuverlässigkeit auftreten können, spreche für die Konzentration auf eine Person als Datenschutzbeauftragte oder Datenschutzbeauftragter innerhalb eines Verbundes auch, dass mit ihr der Gefahr widerstreitender Interessenlagen der einzelnen dazugehörenden Stellen entgegengewirkt werden könne. Vorbehaltlich einer Rückäußerung von uns war der gemeinsame Datenschutzbeauftragte der GeNo und des Klinikums Bremen-Mitte mit diesem Amt bereits auch durch das Klinikum Links der Weser und einer anderen zum Verbund gehörenden Stelle bestellt worden.

Auch nach der schriftlichen Stellungnahme der GeNo verbleiben wir bei unserer Auffassung, dass die gleichzeitige Übertragung der Funktion der oder des Datenschutzbeauftragten durch die GeNo und andere zum Verbund gehörende Stellen mit den datenschutzrechtlichen Vorschriften nicht zu vereinbaren ist. Die nach diesen Vorschriften erforderliche Trennung der Verantwortlichkeiten von Auftraggeber und Auftragnehmer ist nicht auf möglicherweise gegenläufige wirtschaftliche Interessen zurückzuführen. Nach § 9 BremDSG hat der Auftraggeber unter anderem die Pflichten, den Auftragnehmer unter Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen und die Einhaltung dieser Maßnahmen bei der Datenverarbeitung zu überwachen. Der Auftragnehmer darf die ihm überlassenen personenbezogenen Daten nur gemäß der Weisungen des Auftraggebers verarbeiten. Hieraus ergeben sich

klar zu trennende Verantwortlichkeiten, die es erfordern, dass die oder der Datenschutzbeauftragte des Auftraggebers nicht auch die oder der Datenschutzbeauftragte des Auftragnehmers ist.

Des Weiteren darf die Mehrfachbestellung einer oder eines gemeinsamen Datenschutzbeauftragten auch innerhalb eines Verbundes nicht dazu dienen, unterschiedliche Interessen der bestellenden Stellen zu überspielen. Die oder der Datenschutzbeauftragte ist hinsichtlich der Erfüllung der ihr oder ihm gesetzlich übertragenen Aufgaben nur gegenüber der sie oder ihn bestellenden Stelle verantwortlich. Interessen anderer Stellen dürfen die gesetzeskonforme Aufgabenwahrnehmung insbesondere nicht beeinträchtigen.

Eine Klärung mit der GeNo im Hinblick auf die Bestellung von Datenschutzbeauftragten im Klinikverbund steht aus.

## 4. Datenschutz durch Technikgestaltung und -bewertung

### 4.1 IT-Sicherheitsmanagement für das Land Bremen

Der Befall einiger Bereiche des Bremer Landesnetzes mit dem Internetwurm „Conficker“ hat zu einer erneuten Diskussion über ein effektives IT-Sicherheitsmanagement innerhalb der bremischen Verwaltung geführt. Nicht ohne Grund, denn mehrere Dienststellen und Eigenbetriebe waren zeitweise von der elektronischen Kommunikation abgeschnitten. Neben vielfältigen Verbreitungswegen, wie etwa E-Mail-Attachments, schlechte Konfiguration von Servern, Windows-Freigaben und so weiter, sind die destruktiven Eigenschaften des Internetwurms von erheblicher datenschutzrechtlicher Bedeutung. Im schlimmsten Fall ist der Wurm in der Lage, die auf befallenen Rechnern gespeicherten Informationen zu durchsuchen und Rechner via Internet zu steuern.

Nach Entdeckung der Schadsoftware wurde zwar sehr viel bewegt, um sie wieder von den Rechnern zu entfernen, es konnte aber nicht abschließend erforscht werden, auf welchen Wegen die Rechner infiziert wurden. Das bedeutet, es kann auch keine zuverlässige Aussage darüber getroffen werden, ob alle Wege zukünftig für solche oder ähnliche Angriffe blockiert sind.

Als Baustein eines umfassenden Sicherheitskonzeptes fehlt ein Antiviruskonzept, das zum Beispiel auf einem Netzplan beruht, der Auskunft über mögliche Infektionswege, zum Beispiel Internetzugänge, Zugänge aus als nicht vertrauenswürdig klassifizierten Netzen, manuelle Wege, gibt. Auch Rechner mit dem höchsten Infektions- und / oder Schadensrisiko sollten erkennbar sein, um sie besonders isolieren beziehungsweise schützen zu können.

Auch der uns im August durch die Senatorin für Finanzen vorgelegte Entwurf eines Informationssicherheitskonzeptes für die Freie Hansestadt Bremen (FHB-Informationssicherheitskonzept) enthält kein allgemein verbindliches Antivirenkonzept – für uns unter anderem ein Hinweis darauf, dass eine schnelle und durchgreifende Reaktion auf diesen aktuellen Sicherheitsvorfall zumindest in Bezug auf die Entwicklung allgemein verbindlicher Standards nicht möglich war. Das Konzept berücksichtigt zwar wesentliche datenschutzrelevante Sicherheitskriterien, kann aber als Leitlinie nur Teil eines umfassenden Sicherheitsmanagements für die bremische Verwaltung sein, da es ohne diesen Zusammenhang kaum wirksam werden kann. Eine wesentliche Änderung gegenüber dem FHB-Informationssicherheitskonzept von 2003 besteht darin, die Verpflichtung der Dienststellen zur Dokumentation der Umsetzung ihrer Sicherheitsstruktur zu erhöhen und den Grad der Umsetzung zu überprüfen. Bei dem Versuch der Durchsetzung unserer datenschutzrechtlichen Anforderungen sind wir häufig auf eine große Akzeptanz getroffen, allerdings wurde genauso häufig auf die nicht vorhandenen personellen und materiellen Ressourcen verwiesen, die es verhindern, sich ausreichend mit dem Spezialgebiet IT-Sicherheit auseinanderzusetzen und entsprechende technische Maßnahmen ergreifen zu können. Sicherheit hat sich zu einem komplexen Spezialgebiet entwickelt und kann nicht neben der Aufrechterhaltung des laufenden Verwaltungsbetriebs bearbeitet werden. Wir halten daher die Erhöhung der Verpflichtungen der Dienststellen unter den bisherigen Bedingungen für wirkungslos.

Datenschutzrechtlich unklar ist weiterhin, wie die im § 9 des Bremischen Datenschutzgesetzes (BremDSG) festgelegte Auftragskontrolle gegenüber den externen Dienstleistern wahrgenommen wird, wie der Aufbau eines zentralen Verzeichnis-

dienstes (Active directory) mit zentralen Sicherheits- und Datenschutzerfordernissen in Übereinstimmung gebracht werden kann, wie Zugriffe von Teilnehmerinnen und Teilnehmern des bremischen Verwaltungsnetzes und von externen Anwenderinnen und Anwendern außerhalb der im Sicherheitskonzept definierten Grenznetze kontrolliert werden können, wie die Zugriffe von Dataport als zentralem Dienstleister in die bremischen Sicherheitsstandards zu integrieren sind und wie die gesamte Sicherheitsstruktur durch eine effektive Revision kontrollier- und steuerbar werden kann.

Wir halten deshalb dringend die Entwicklung eines Konzeptes zum IT-Sicherheitsmanagement in Abstimmung mit den Ressorts und die Berücksichtigung des hierfür erforderlichen Aufwands für die Einführung und den laufenden Betrieb in zukünftigen Produktplänen für notwendig. Wesentlicher Bestandteil muss die Einrichtung einer zentral für das Sicherheitsmanagement in Bremen verantwortlichen Stelle sein, die für die effiziente Erarbeitung, Fortschreibung, Veröffentlichung und Umsetzung von IT-Sicherheitskonzepten unter Berücksichtigung der Wechselwirkung zentraler und dezentraler Sicherheit zuständig ist. Weitere Aufgaben sind unter anderem der Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit und deren Aufrechterhaltung, die Durchführung erforderlicher Risikoanalysen und die Entwicklung von Konzepten und Maßnahmeplänen beim Eintreten von datenschutzrechtlich und sicherheitstechnisch relevanten Vorfällen. Darüber hinaus ist eine wirksame Kontrolle der Umsetzung definierter Sicherheitsziele unabdingbar.

Im Entwurf des FHB-Informationssicherheitskonzeptes wird festgelegt, dass sich das IT-Management des bremischen Verwaltungsnetzes zukünftig an allgemein verbindlichen Standards orientieren soll. Es wird ein Werkzeug benötigt, das ein strukturiertes Sicherheitsmanagement unterstützt. Es muss Hilfestellung beim Aufbau entsprechender Strukturen aus organisatorischer, personeller, infrastruktureller und technischer Hinsicht bieten, den Aufbau eines transparenten IT-Managements und die Verknüpfung zentraler und dezentraler Sicherheitsstrukturen ermöglichen.

Der Senat hat mit Beschluss vom 29. September 2009 unter anderem die Neueinrichtung eines IT-Management-Ausschusses (ITA) und einer IT-Steuerungsgruppe (ITSG) beschlossen. Diese Gremien sind in erster Linie Entscheidungsgremien. Der ITA entscheidet zwar über das Sicherheitskonzept und IT-Regelwerk, kann aber nicht die erforderlichen Managementaufgaben selbst übernehmen.

Ein effektives Sicherheitsmanagement benötigt aus unserer Sicht zur Bewältigung der komplexen Aufgaben zusätzliche Ressourcen. Letztendlich bedeutet eine effektive Sicherheitsstruktur auch eine effiziente IT-Organisation, sodass der Aufwand hierfür durchaus verhältnismäßig ist – und somit auch ökonomisch.

### 4.2 Administrativer Zugang am Dataport-Standort Bremen

Mitte des letzten Jahres wurden uns von der Senatorin für Finanzen Unterlagen der Anstalt des öffentlichen Rechts Dataport zugeleitet, in denen die Möglichkeit aufgezeigt wurde, über einen einheitlichen und revisionssicheren Weg Administrationstätigkeiten in Bremen von einer sogenannten Admin-Area vorzunehmen (vergleiche 31. Jahresbericht, Ziffer 6.4). Die eingereichte Dokumentation enthielt noch einige offene Fragestellungen, deren Klärung bisher nicht erfolgt ist. Auch in diesem Jahr wurde uns kein überarbeitetes Administrationskonzept von Dataport vorgelegt.

In der Stellungnahme des Senats wurde mitgeteilt, dass der administrative Zugang von der Senatorin für Finanzen nicht freigeschaltet wurde. Wir gehen derzeit davon aus, dass nun im nächsten Berichtsjahr die Vorlage eines Konzeptes erfolgt, in dem beispielsweise Themen wie die Protokollierung und Revision sicherheitskritischer administrativer Tätigkeiten, Rechte zugreifender Administratoren, Sicherheitsniveau der eingesetzten Anmeldeverfahren sowie die „bremenspezifische“ Umsetzung berücksichtigt sind.

### 4.3 VIS – Zentrales System zur elektronischen Aktenführung

Im Rahmen der Bewertung der Nutzung von VISkompakt im Projekt „Stopp der Jugendgewalt“ (vergleiche Ziffer 5.2 dieses Berichts) haben wir eine Datenschutzdokumentation für das System VISkompakt angefordert, das als zentrales Dokumentenmanagementsystem in der bremischen Verwaltung eingesetzt wird und mit dem sensible personenbezogene Daten verarbeitet werden. Die Senatorin für Finanzen hat Dataport mit der Datenverarbeitung für diese Anwendung beauftragt.

Als Dokumentation wurde uns eine Leistungsbeschreibung übersandt, die die Leistungsbeziehung zwischen der Senatorin für Finanzen und Dataport beschreibt. Dieses Dokument war nicht auf einem aktuellen Stand und ersetzte zudem nicht die notwendige Datenschutzdokumentation nach dem Bremischen Datenschutzgesetz (BremDSG).

Festzulegen ist, für welche Bereiche die Senatorin für Finanzen als Auftraggeberin der Basiskomponente verantwortlich ist und welche Verantwortung die einzelnen Dienststellen als Eigentümerinnen der Daten übernehmen. Dies betrifft unter anderem die Infrastruktur, das Administrationskonzept, Berechtigungskonzepte und die VIS-Geschäftsprozesse.

Im Frühjahr des Berichtsjahres hatten wir daher um die Übersendung des Rahmendatenschutzkonzeptes, der Berechtigungskonzepte sowie ergänzender Dokumentationen gebeten. Da auch sehr sensible personenbezogene Daten verarbeitet werden, haben wir sowohl eine Verschlüsselung auf dem Übertragungsweg wie auch bei der Datenspeicherung gefordert. Weitere Fragestellungen und Anforderungen ergaben sich zur Verpflichtung auf das Datengeheimnis, zur Auftragsdatenverarbeitung sowie zur Bearbeitung von Verschlusssachen.

Ende des Jahres haben wir die Leistungsbeschreibung „Zentrale Infrastruktur für VISkompakt Bremen“ nebst weiteren Anlagen erhalten. Das noch ausstehende Datenschutz- und Sicherheitskonzept wurde uns für Februar 2010 angekündigt. Dazu werden wir im kommenden Berichtsjahr Stellung nehmen.

## 5. Inneres

### 5.1 „Künstliche DNA“

Die Polizei Bremen startete im Berichtsjahr ein Projekt mit dem Namen „Eigentumsschutz durch künstliche DNA“. Sie kooperiert dazu mit einer privaten Firma, die entsprechende Produkte vertreibt. Die „künstliche DNA“ ist eine fluoreszierende Flüssigkeit, die ähnlich einem Lack auf Gegenstände aufgebracht wird und dem Diebstahlschutz dienen soll. Die Substanz färbt nach dem Trocknen nicht mehr ab und kann mit Hilfe einer UV-Lampe sichtbar gemacht werden. Das Produkt ist in einem Fläschchen erhältlich, das zum Markieren von ungefähr 70 Gegenständen ausreicht. Jedes Fläschchen ist mit einem eigenen DNA-Code sowie mit mikroskopisch kleinen Kunststoffplättchen, den sogenannten Microdots, versehen, um die Zuordnung des markierten Gegenstands zur Eigentümerin oder zum Eigentümer zu ermöglichen. In die Microdots sind einmalige Zifferncodes eingraviert, die mit Hilfe eines Mikroskops sichtbar werden. Haben sich die Eigentümerin oder der Eigentümer des Gegenstandes in der Kundendatenbank der Herstellerfirma registrieren lassen, kann die Polizei diese im Fall eines Diebstahls über die Datenbank ermitteln und den gestohlenen Gegenstand zurückgeben.

In der ersten Phase des Projektes der Polizei Bremen, die im Oktober des Berichtjahres begann, wurden Fläschchen mit der „künstlichen DNA“ an Schulen verteilt, um dort Wertgegenstände zu kennzeichnen. Die zweite Phase startete im November. In dieser Phase wurden die Bewohnerinnen und Bewohner zweier Stadtteile in Bremen und Bremerhaven von der Polizei mit kostenlosen Fläschchen mit der Flüssigkeit, inklusive einer UV-Taschenlampe in Form eines Schlüsselanhängers, ausgestattet. Zugleich wurden Schilder in den betreffenden Gebieten angebracht, die darauf hinweisen, dass die Häuser und Wohnanlagen „DNA-gesichert“ seien.

Vom rechtlichen Aspekt her haben wir gegen den beschriebenen Einsatz der Flüssigkeit zum Diebstahlsschutz keine Bedenken. Bezüglich der Herstellerdatenbank zur Registrierung von Verwendern der „künstlichen DNA“ haben wir dagegen datenschutzrechtliche Probleme festgestellt. Der Zugriff auf die Datenbank durch die Polizei Bremen erfolgt über das Internet. Nachdem zunächst unklar war, ob die Daten verschlüsselt übertragen werden, teilte die Polizei Bremen uns zwischenzeitlich mit, dass die Internetseite zur Eingabe der Kundendaten eine verschlüsselte Übertragung der Daten ermöglicht. Die Zuständigkeit zur Prüfung dieser Internetanwendung, beispielweise bezüglich der Maßnahmen zur Absicherung gegenüber Angriffen aus dem Internet, liegt bei der datenschutzrechtlichen Kontrollbehörde des Bundeslandes Baden-Württemberg. Wir haben dorthin entsprechende Informationen weitergegeben. Über diese Bedenken hinaus besteht ein Missbrauchspotenzial mit der DNA-Flüssigkeit. Fremde Gegenstände könnten als ei-

gene markiert werden. Nicht abschließend geklärt ist zudem, wie mit den Eintragungen in der Datenbank bei rechtmäßiger Veräußerung von Gegenständen verfahren wird.

In der dritten Phase des Projektes sollen nicht Gegenstände, sondern Menschen mit der „künstlichen DNA“ markiert werden. Es sollen mit der DNA-Flüssigkeit ausgestattete Sprühanlagen in Tankstellen und Sparkassen installiert werden. Vermeintliche Täterinnen oder Täter sollen beim Verlassen des Gebäudes mit der DNA-Flüssigkeit besprüht werden, die mehrere Wochen auf der Haut haftet. Das Auslösen des Spraymechanismus erfolgt beispielsweise durch eine jeweils aktivierbare Lichtschranke.

Wir haben erhebliche datenschutzrechtliche Bedenken im Hinblick auf den Einsatz der Sprühanlagen durch Private. Nach unserer Auffassung stellt das Markieren von Personen einen erheblichen Grundrechtseingriff dar, für den als Maßnahme der Strafverfolgung keine Rechtsgrundlage existiert. Die einzige Rechtsgrundlage zur Strafverfolgung durch Bürgerinnen und Bürger ist das einstweilige Festnahmerecht nach § 127 Absatz 1 der Strafprozessordnung (StPO), das hier nicht greift. Technische Fehler, etwa bei der Auslösung des Sprays oder unbeabsichtigte Fehlbedienungen, können nicht ausgeschlossen werden. Somit ist es möglich, dass Personen fälschlich markiert werden. Ein versehentliches Mitbesprühen von unbeteiligten Personen ist ebenso denkbar wie absichtliche Missbrauchsfälle. Eine fälschliche Brandmarkung als Straftäterin oder Straftäter wäre die Folge. Aufgrund der weiten Verbreitung der „entlarvenden“ UV-Lampen durch und nach der zweiten Phase des Projektes handelte es sich sogar um eine öffentliche Stigmatisierung.

Der Senator für Inneres und Sport hat nach einem Gespräch mit der Landesbeauftragten für Datenschutz und Informationsfreiheit angekündigt, dass der Einsatz der DNA-Sprühanlagen bei privaten Einrichtungen künftig unter der „Schirmherrschaft“ beziehungsweise beratenden Begleitung der Polizei stattfinden wird. Der Betreiber einer solchen DNA-Sprühanlage müsse sich gegenüber der Polizei verpflichten,

— die Anlage nach bestimmten Kriterien anzubringen,

— bestimmte Auslösevorrichtungen zu verwenden sowie

— eine Schulung oder Unterweisung der Mitarbeiterinnen und Mitarbeiter durchzuführen.

— Zudem sind Hinweisschilder deutlich sichtbar in einer bestimmten Mindestgröße anzubringen.

Die Vertriebsfirma der DNA-Sprühanlagen werde diese nur an Firmen weitergeben, für die eine Unbedenklichkeitsbescheinigung der Polizei vorliege. Die Informationen über Firmen mit DNA-Sprühanlagen würden im Leitrechner der Polizei gespeichert, um bei Einsatzanlässen die Streifenwagen schon auf der Anfahrt zu informieren.

Die hierin liegende Übernahme einer größeren polizeilichen Verantwortung für den Einsatz der Sprühanlagen durch Private halten wir für einen wichtigen Schritt. Gleichwohl vermag auch sie aus unserer Sicht keine gesetzliche Rechtfertigung für die Besprühung von Menschen durch Private zum Zwecke der Strafverfolgung zu begründen.

### 5.2 „Stopp der Jugendgewalt“

In der Koalitionsvereinbarung für die 17. Wahlperiode wurde vor dem Hintergrund einer zunehmenden Anzahl von durch Jugendliche und Heranwachsende begangenen Gewaltdelikten vereinbart, dass Innen-, Justiz-, Sport-, Jugend- und Bildungsressort noch im Jahr 2007 ein gemeinsames Handlungskonzept „Stopp der Jugendgewalt“ vorlegen. In dem Konzept sollen unterschiedliche Ansätze und Möglichkeiten der beteiligten Ressorts zu einem wirksamen Maßnahmenbündel zusammengefasst werden. Das Ziel der Maßnahmen besteht darin, jugendliche Täterinnen und Täter, die bereits einige Male in Erscheinung getreten sind, von einer kriminellen Karriere abzuhalten. In der Zwischenzeit wurden eine Reihe von Handlungsanleitungen für einzelne Projekte erstellt, die zahlreiche datenschutzrechtliche Probleme und Bedenken aufwerfen. Hierüber befinden wir uns in der Diskussion mit dem Senator für Inneres und Sport als dem federführenden Ressort, aber auch mit den anderen beteiligten Ressorts (vergleiche dazu auch Ziffer 7.2 dieses Berichts).

**Personenorientierte Berichte**

Bei den personenorientierten Berichten handelt es sich um eine Zusammenfassung seitens der Staatsanwaltschaft und der Polizei gesammelter Erkenntnisse über jugendliche oder heranwachsende Intensivtäterinnen oder -täter; zum Begriff siehe unten. Ziel der ressortübergreifenden Berichte ist es, einen umfassenden Gesamtlebenslauf zu erhalten, der fortlaufend aktualisiert wird, um so schnell und wirkungsvoll Interventionen einzuleiten. Zudem sollen geeignete präventive Maßnahmen für einzelne Personen aufgezeigt werden. Der Bericht wird als Sonderheft Bestandteil der Ermittlungsakte. Für die Bearbeitung der Daten soll das Computerprogramm VISkompakt genutzt werden, das die Senatorin für Finanzen als zentralen Dienst für das Bremische Verwaltungsnetz zur Verfügung stellt (vergleiche Ziffer 4.3 dieses Berichts).

Unsere auf die Anwendung der Rechtsgrundlagen bezogenen Bedenken sind durch eine Überarbeitung des Konzeptes, nach der insbesondere nur noch an der Strafverfolgung beteiligte Einheiten auf die Daten zugreifen dürfen, zwischenzeitlich weitestgehend ausgeräumt worden.

Aus datenschutzrechtlicher Sicht verbleiben allerdings Probleme bei der technischen Umsetzung. Bis zum Einsatz von VISkompakt sollen die Berichte in einem polizeiinternen Laufwerk als einfache Textdateien bearbeitet werden. Wir äußerten gegen das vorgelegte Konzept etliche datenschutzrechtliche Bedenken. So erfolgte beispielsweise keine revisionssichere Protokollierung der Berechtigungsvergabe. Wir wiesen darauf hin, dass unabhängig davon eine lückenlose Dokumentation der Berechtigungsvergabe durch die Verantwortlichen erforderlich ist. Die Speicherung der personenorientierten Berichte erfüllte weiterhin nicht die Vorgabe des Bremischen Datenschutzgesetzes bezüglich der Eingabekontrolle. Datenschutzrechtlich problematisch war auch die Regelung der Zugriffskontrolle. Daneben fehlten detaillierte Angaben zur Weitergabekontrolle. Die Speicherung der Daten bei der Polizei auf dem Laufwerk war als Übergangslösung gedacht, die nun von einer Verarbeitung der Daten unter VISkompakt abgelöst werden soll.

Zur geplanten Nutzung des VIS-Systems liegt uns derzeit noch kein zentrales Datenschutz- und Sicherheitskonzept vor. Voraussetzung für die Nutzung des Systems zur Speicherung der personenorientierten Berichte ist der verschlüsselte Zugriff auf die Daten auf dem Leitungsweg sowie die verschlüsselte Speicherung der Daten auf den Servern. Des Weiteren muss ein geeignetes Berechtigungskonzept für den Zugriff über den VIS-Mandanten auf den dargestellten VIS-Geschäftsprozess erstellt werden. Vor Einsatz von VISkompakt müssen geeignete technische und organisatorische Maßnahmen getroffen werden. Dahingehend werden wir noch eine datenschutzrechtliche Prüfung vornehmen.

**Behördenübergreifende Fallkonferenzen**

Laut Konzept dient eine behördenübergreifende Fallkonferenz im Sinne einer Ultima Ratio als Instrument zur Verstärkung staatlichen Handelns. Durch die gemeinsame Analyse und Bewertung des Sachverhalts und der bisherigen Maßnahmen soll einerseits festgestellt werden, weshalb die bisherigen Hilfen und Interventionen nicht erfolgreich waren und andererseits nach abgestimmten Lösungen gesucht werden. Voraussetzung für die Einberufung einer behördenübergreifenden Fallkonferenz ist, dass die Abwehr der Gefahr nicht allein mit den eigenen Ressourcen realisiert werden kann.

Wir haben hinsichtlich der Durchführung von behördenübergreifenden Fallkonferenzen erhebliche datenschutzrechtliche Bedenken geäußert. Innerhalb der Fallkonferenzen soll an einem runden Tisch ein umfangreicher Austausch von personenbezogenen, teilweise sensiblen Daten der betroffenen Personen zwischen den Vertreterinnen und Vertretern der beteiligten Behörden stattfinden, für den größtenteils keine Rechtsgrundlage existiert. Daher diskutieren wir gegenwärtig mit dem Senator für Inneres und Sport und dem Senator für Justiz und Verfassung eine Variante, nach der die Übermittlung der Informationen auf eine Einwilligung der Betroffenen gestützt werden soll. Folgende Aspekte haben wir in diese Diskussion eingebracht: Zunächst einmal ist zweifelhaft, ob eine Einwilligung überhaupt als weiterer Erlaubnistatbestand für einen Eingriff auf das Recht auf informationelle Selbstbestimmung neben die bestehenden – oder auch bewusst nicht bestehenden – gesetzlichen Regelungen treten kann. Auch die Freiwilligkeit der Einwilligung kann im öffentlichen Bereich fragwürdig sein. Sofern gleichwohl eine Einwilligungs-

lösung praktiziert werden soll, müssen an die Einwilligung bestimmte Anforderungen gestellt werden. So sind die Betroffenen beispielsweise in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Zweck der Datenverarbeitung und, bei einer beabsichtigten Übermittlung, auch über die Empfänger aufzuklären. Zudem sind die Betroffenen unter Hinweis auf die möglichen Rechtsfolgen darauf hinzuweisen, dass die Einwilligung verweigert und mit Wirkung für die Zukunft widerrufen werden kann. Die Einwilligung müsste dann eingeholt werden, wenn die zuständige Stelle entschieden hat, dass eine Fallkonferenz angezeigt ist. Das Gesetz gibt sich nicht mit einer Zustimmung, die an keinen Zeitpunkt gebunden ist, zufrieden.

Problematisch ist zudem der Kreis der Teilnehmerinnen und Teilnehmer. Es ist noch nicht abschließend geklärt, ob neben Vertreterinnen und Vertretern der Polizei Bremen, des Amtes für Soziale Dienste beziehungsweise des Jugendamtes sowie der zuständigen Schule auch die Staatsanwaltschaft und die Ausländerbehörde an den Konferenzen teilnehmen dürfen. Der geplante Austausch der Daten kann für die Betroffenen weitreichende Folgen haben. So sind beispielsweise die Ermittlungsbehörden aufgrund des Legalitätsprinzips verpflichtet, bei Vorliegen von hinreichenden tatsächlichen Anhaltspunkten wegen aller verfolgbaren Straftaten einzuschreiten. Die betroffenen Jugendlichen müssen daher darüber informiert werden, dass ihre Einwilligung in eine Fallkonferenz gegebenenfalls die Einleitung eines Strafverfahrens zur Folge haben kann. Dieser Aspekt wurde bei der Beurteilung der Einwilligungsfähigkeit berücksichtigt.

Über die endgültigen Formulierungen der Handlungsanleitung und der Einwilligungserklärung für die Fallkonferenzen befinden wir uns noch in der Diskussion mit den zuständigen Ressort.

**Intensivtäterkonzept**

Als Intensivtäterinnen und -täter werden in Bremen Personen definiert, die durch gewohnheits- oder gewerbsmäßige Begehung von Straftaten mit Schwerpunkt in den Bereichen Eigentums- und Gewaltkriminalität aufgefallen sind und bei denen angenommen werden kann, dass sie weitere Straftaten verüben werden. Eine Altersgrenze besteht nicht. Im Rahmen des Intensivtäterkonzeptes ist die Erstellung einer Intensivtäter-Ranking-Liste und eine Intensivtäterdatei vorgesehen. Die Einordnung der Täter in die Ranking-Liste erfolgt im Wege der Gewichtung der begangenen Taten durch festgelegte Multiplikatoren sowie aufgrund von Erkenntnissen, die sich aus der Hellfeld-Analyse in Kombination mit der erfahrungsgestützten Einschätzung des Dunkelfeldes und nicht aufgeklärter Straftaten herleiten lassen. Darüber hinaus ist die Einordnung einer Person als Intensivtäterin oder -täter auch bei ausreichender Negativprognose möglich. Die Intensivtäterdatei enthält zahlreiche Informationen über die Betroffenen und soll in das Intranet der Polizei eingestellt werden. Es soll ein behördenübergreifender Informationsaustausch mit dem Ziel der Unterbrechung der kriminellen Karriere stattfinden. Kooperationen mit anderen Behörden und Bearbeitung der Fälle an runden Tischen sind geplant.

Wir haben die Polizei Bremen darauf hingewiesen, dass sowohl für die Intensivtäterlisten als auch die Intensivtäterdatei eine Verfahrensbeschreibung gemäß § 8 BremDSG sowie ein Datenschutzkonzept erforderlich sind. Wir werden die Unterlagen umfassend prüfen, sobald sie uns von der Polizei zur Verfügung gestellt worden sind.

**Schwellentäterkonzept**

Das zwischen dem Senator für Inneres und Sport, der Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales und dem Senator für Justiz und Verfassung vereinbarte Schwellentäterkonzept wendet sich an straffällig gewordene Jugendliche und Heranwachsende, die als Mehrfachtäterinnen und Mehrfachtäter aufgefallen sind und bei denen sich abzeichnet, dass sie auch weiterhin Straftaten begehen werden, sie sich also am Anfang einer kriminellen Karriere befinden. Das Ziel des Konzeptes liegt darin, die Anzahl der Straftaten, insbesondere der Gewalttaten durch Jugendliche und Heranwachsende, zu reduzieren. Das Konzept basiert unter anderem auf der Grundannahme, dass die Verfestigung von kriminellen Entwicklungen reduziert werden kann, wenn es gelingt, durch fortgesetztes Fehlverhalten entstehende Entwicklungsgefährdungen frühzeitig zu erkennen und durch verhaltenskorrigierende Interventionen und Hilfen sowie begleitende Maßnahmen zu reagieren. Zur strukturierten Information der Beteiligten über ein möglicherweise ge-

steigertes Risiko künftigen kriminellen Verhaltens wurde ein Formblatt entwickelt. Staatsanwaltschaft, Jugendgericht und Jugendhilfe ergreifen in geeigneten Fällen und, soweit es die gesetzlichen Vorschriften zulassen, bei Verfahren gegen Schwellentäter im Rahmen ihrer Zuständigkeit geeignete Maßnahmen. Die Kooperationsvereinbarung zur Umsetzung des Konzeptes wurde auf Grundlage eines Projektberichts des Amtes für Soziale Dienste, der Polizei Bremen, der Staatsanwaltschaft Bremen und des Amtsgerichts Bremen, Jugendgericht, unter Berücksichtigung unserer Anmerkungen erstellt. Zurzeit wird das Handlungskonzept von uns datenschutzrechtlich geprüft.

**Interventionsteams**

Der Auftrag von Interventionsteams besteht nach der Kooperationsvereinbarung zwischen der Polizei Bremen, dem Amt für Soziale Dienste Bremen sowie dem Landesinstitut für Schule Bremen darin, unter ressortübergreifender Abstimmung auf Gewaltphänomene in Schulen und sonstigen öffentlichen Räumen zeitnah zu reagieren und Gefährdungslagen unmittelbar zu beseitigen. Dazu werden ressortübergreifend besetzte Fachteams gebildet, die eine fallübergreifende Situationsanalyse und -bewertung durchführen und anlassbezogen sowie situativ und zeitlich begrenzt tätig werden. Das Ziel besteht in einer unmittelbaren Auflösung der Problemlage, einer kurzfristigen koordinierten Deeskalation, der Sicherstellung von Interventions- und Hilfestrategien sowie der Entwicklung von Problemlösungsansätzen. Es sollen akute Gewalt- und Problemlagen mit den Täterinnen und Tätern, Problembeteiligten und Opfern unter Einbeziehung betroffener Lehrkräfte, Schulleitungen und Sorgeberechtigter aufgearbeitet werden. Die bereichsspezifisch festgelegte Fallzuständigkeit für die Gewährung von Hilfen und Leistungen oder die Durchführung von Verfahren bleibt von dem Konzept unberührt. Eine Beteiligung weiterer Fachdienste ist im Einzelfall vorgesehen. Die Kooperationsvereinbarung legt fest, dass der Austausch personenbezogener Daten grundsätzlich in Kenntnis und mit Zustimmung der Betroffenen erfolgt. Die Übermittlung personenbezogener Daten ohne entsprechende Einwilligung soll zur unmittelbar zweckgebundenen Gefahrenabwehr bei Selbst- oder Fremdgefährdung sowie im Rahmen der Kindeswohlsicherung nach den Bestimmungen des Sozialgesetzbuches (SGB) VIII im Rahmen und auf Grundlage der Übermittlungsbefugnisse des Bremischen Schulgesetzes, auf Grundlage der polizeilichen Mitteilungsbefugnisse nach dem Bremischen Polizeigesetz sowie im Rahmen und auf Grundlage der Befugnisnorm nach § 34 Strafgesetzbuch (StGB) und unter Beachtung des § 203 StGB soweit und in dem Umfang, in dem dies zur unmittelbaren Abwendung und Beseitigung der Problemlage erforderlich ist, zulässig sein.

In einem ersten Gesprächstermin mit Vertreterinnen und Vertretern der Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales baten wir um eine Präzisierung der geplanten Datenverarbeitung, die sich nicht eindeutig aus der Projektbeschreibung ergibt. Inhaltlich äußerten wir ähnliche Bedenken wie beim Konzept zu den behördenübergreifenden Fallkonferenzen. Das Konzept bedarf noch einer umfassenden datenschutzrechtlichen Prüfung, sobald die von uns angeforderten Informationen vollständig vorliegen.

### 5.3 Verwendung des personenbezogenen Hinweises „psychisch auffällig“ durch die Polizei Bremen

Personenbezogene Hinweise (PHW) dienen in erster Linie der Eigensicherung der Polizei und werden im Rahmen der Einsatztaktik berücksichtigt. PHW sind beispielsweise Merkmale wie „gewalttätig“, „bewaffnet“ oder „psychisch auffällig“. Der letztgenannte PHW wurde bundesweit nur im Land Bremen nach der Dienstanweisung über polizeiliche Maßnahmen gegenüber psychisch auffälligen Personen aus dem Jahr 2003 vergeben. Eine Verwendung des Merkmals ist danach möglich, ohne dass eine psychische Krankheit durch einen Arzt festgestellt wurde. Im 30. Jahresbericht, Ziffer 9.5 und Ziffer 9.19, sowie im 31. Jahresbericht, Ziffer 9.6, wiesen wir auf die Gefahr einer Stigmatisierung der Betroffenen durch die Verwendung dieses PHW hin. Fehler bei der Vergabe können schwerwiegende Konsequenzen nach sich ziehen. Für die Betroffenen ist es sehr schwierig, den Hinweis korrigieren oder löschen zu lassen.

Aufgrund dieser Bedenken wird nun nach Auskunft des Ressorts von der Polizei der PHW „psychisch auffällig“ nicht mehr vergeben. Künftig wird nur noch das Merkmal „psychisch krank“ verwendet, das der Feststellung einer psychischen Erkran-

kung durch einen Facharzt bedarf. Ungeklärt ist derzeit noch der Umgang mit den sogenannten Altfällen, in denen der PHW „psychisch auffällig“ bereits gespeichert ist. Eine Arbeitsgruppe unter Beteiligung der Ressorts Gesundheit, Justiz und Inneres soll hierzu eine Lösung erarbeiten. Es ist vorgesehen, das Ergebnis mit der Landesbeauftragten für Datenschutz und Informationsfreiheit abzustimmen.

### 5.4 Projekt der Bremer Polizei „Senioren im Straßenverkehr“

Im September 2009 rief uns ein älterer Bürger empört an und beschwerte sich über das Vorgehen der Polizei. Dieser Beschwerde lag folgender Sachverhalt zugrunde: Anlässlich eines Verkehrsunfalls eines älteren Bürgers wurde im Rahmen der Ahndung einer Ordnungswidrigkeit nach §§ 1 Absatz 2, 49 Absatz 1 Nummer 1 Straßenverkehrs-Ordnung, § 24 Straßenverkehrsgesetz, nach einem Familienangehörigen als Ansprechpartner geforscht, um den freiwilligen Verzicht auf die Fahrerlaubnis des älteren Bürgers anzuregen und um langwierige verwaltungsrechtliche Maßnahmen der Fahrerlaubnisbehörden überflüssig zu machen.

Ein Polizist hatte bei der Schwiegertochter dieses in Rede stehenden Senioren angerufen und sich mit ihr über einen Verkehrsunfall unterhalten, an dem der ältere Bürger beteiligt gewesen war. Der Verkehrspolizist wollte die Einschätzung der Schwiegertochter über die geistige Fähigkeit des betroffenen Senioren hinsichtlich dessen Verhalten im Straßenverkehr herausfinden.

Nach einem umfangreichen Schriftwechsel mit der Polizei stellte sich heraus, dass dieser Anruf im Rahmen eines Pilotprojektes „Überprüfung von Verkehrsunfällen unter Beteiligung von Senioren als Verursacher oder Mitverursacher hinsichtlich möglicher fahrerlaubnisrelevanter Befähigungsbedenken“ getätigt wurde. Dieses Pilotprojekt startete im September 2008 und wird fortgeführt. Es betrifft präventivpolizeiliche Maßnahmen im Zusammenhang mit verhaltensauffälligen, älteren Verkehrsteilnehmern nach atypischen Verkehrsunfällen.

Zur Ermittlung des Namens und der Telefonnummer des Familienangehörigen wurde eine automatisierte Abfrage im Meldewesen (sogenannte Meso-Abfrage) hinsichtlich des älteren Verkehrsteilnehmers durchgeführt. Eine Meso-Abfrage zur Ermittlung der aktuellen Adressdaten eines Verkehrsteilnehmers oder auch zur Feststellung der Identität einer Person zur Erforschung einer Ordnungswidrigkeit gemäß § 53 Gesetz über Ordnungswidrigkeiten ist grundsätzlich zulässig. Im vorliegenden Fall jedoch sollte die Meso-Abfrage nicht dem Zweck der Adress- oder Identitätsermittlung des beteiligten Verkehrsteilnehmers – denn diese stand fest –, sondern vielmehr der Ermittlung eines Angehörigen dienen. Die Meso-Abfrage zu diesem Zweck war im vorliegenden Fall datenschutzrechtlich unzulässig.

Aufgrund des Namens und des Geburtsdatums der unter der gleichen Adresse wie der ältere Verkehrsteilnehmer in der Vergangenheit gemeldeten Person wurde der Schluss auf die Familienangehörigkeit – Sohn des Betroffenen – gezogen. Nun wurde die Telefonnummer des Familienangehörigen aus dem Telefonbuch entnommen und bei ihm angerufen. Allerdings war der Sohn des betroffenen Verkehrsteilnehmers nicht zuhause, sondern dessen Ehefrau ging an das Telefon. Die Mitteilung an sie, dass ihr Schwiegervater einen Verkehrsunfall hatte, war ebenfalls datenschutzrechtlich unzulässig.

Das Konzept der Polizei Bremen wurde mittlerweile datenschutzgerecht gestaltet und sieht nach dem internen Ergebnisbericht aus Januar 2009 nunmehr vor, mit Angehörigen nur nach ausdrücklicher Zustimmung beziehungsweise im Beisein des betroffenen älteren Verkehrsteilnehmers ein Gespräch über Befähigungszweifel im Straßenverkehr zu führen. Es ist damit konzeptionell datenschutzkonform. Die Polizei Bremen versicherte uns, in den angesprochenen Fällen datenschutzgerecht und im Einvernehmen mit den betroffenen Bürgerinnen und Bürgern zu handeln.

### 5.5 Weitergabe einer Mobiltelefonnummer durch die Polizei Bremen

Ein Petent teilte uns mit, dass er in einen Verkehrsunfall verwickelt gewesen sei. Die Polizei habe ihn dazu vernommen, wobei er die Mobiltelefonnummer, unter der er zu erreichen sei, angegeben habe. Einige Zeit später sei er auf dem Handy von einer durch den Unfall geschädigten Person angerufen worden. Der Petent vermutete, dass die Polizei Bremen seine Mobiltelefonnummer weitergegeben habe, womit er nicht einverstanden gewesen sei. Wir nahmen daraufhin vor Ort Einsicht in die Protokolldaten über die Abrufe der personenbezogenen Daten des Petenten

aus dem polizeilichen Informationssystem, um zu überprüfen, wer Zugriff auf die Daten hatte. Die Auswertung der Protokolldaten ergab, dass mehrere Polizistinnen und Polizisten während des in Betracht kommenden Zeitraums auf die Daten zugegriffen hatten.

Wir baten daraufhin den behördlichen Datenschutzbeauftragten der Polizei Bremen, sich an die infrage kommenden Polizeibeamtinnen und Polizeibeamten zu wenden, um herauszufinden, wer die Mobilfunknummer an die geschädigte Person herausgegeben hatte und diesen auf die datenschutzrechtlichen Vorschriften aufmerksam zu machen. Zudem haben wir darauf hingewiesen, dass zum Zwecke der Sensibilisierung für diese Problematik eine Information der Polizei Bremen insgesamt erforderlich ist. Mobil- und Festnetznummern von Personen dürfen grundsätzlich nicht an Dritte weitergegeben werden. Insbesondere kann keine konkludente Einwilligung in die Weitergabe unterstellt werden.

### 5.6 Vermeintliche Halterabfrage eines Pkw-Kennzeichens

Im Sommer des Berichtsjahres wandten sich zwei Angehörige des öffentlichen Dienstes an uns und äußerten den Verdacht, dass ihr Privatleben seitens ihrer Vorgesetzten ausspioniert würde und dass diese unbefugte Halterabfragen anhand der Kennzeichen ihrer privaten Pkw vorgenommen hätten. Die betroffenen Personen leben in Bremen zusammen in einer Wohngemeinschaft. Einer der Petenten ist beruflich in Niedersachsen tätig. Der Landesbeauftragte für den Datenschutz Niedersachsen hat uns gegenüber bestätigt, dass in Niedersachsen entsprechende Halterabfragen durchgeführt wurden. Wir ließen uns daraufhin die Daten der Protokollierung über ZEVIS-Abfragen (Zentrales Verkehrsinformationssystem beim Kraftfahrtbundesamt Flensburg) und eKOL-Abfragen (komfortable Lösung zur Abfrage und Recherche von ZEVIS-Daten) mitteilen. Daraus ergab sich jedoch, dass hinsichtlich der betreffenden Kennzeichen weder von der Polizei noch vom Stadtamt Bremen Abfragen durchgeführt worden waren. Das Ergebnis teilten wir den Petenten mit.

### 5.7 Datenschutzkonzepte bei der Polizei Bremen

In diesem Berichtsjahr hat die Polizei Bremen uns ihren Entwurf des Rahmendatenschutzkonzeptes übersandt, das sich derzeit in unserer Prüfung befindet. Weiterhin wurden wir bei der Bewertung verschiedener Fachverfahren beteiligt. Derzeit gibt es noch Klärungsbedarf zu den Speicherfristen beim Verfahren des Einsatzleitsystem FELIS (Flexibles Einsatzleitsystem Innere Sicherheit) zur Datenübermittlung von Passagierlisten an die Wasserschutzpolizei sowie zum Einsatz des Verfahren PIER (Polizeiliche Information Ermittlung Recherche) für besonders sensible Daten. Weiterhin teilte uns die Polizei Bremen mit, dass sie die Einführung eines Vorgangsbearbeitungssystems plant. Dazu haben wir im Vorfeld die datenschutzrechtlichen Anforderungen mitgeteilt. Wir gehen davon aus, dass wir bei dem Einführungsprozess beteiligt werden.

### 5.8 Datenschutzkonzepte beim Stadtamt Bremen

Im 29. Jahresbericht hatten wir über das Fehlen eines allgemeinen Rahmendatenschutzkonzeptes beim Stadtamt Bremen berichtet. Das allgemeine Rahmendatenschutzkonzept sowie das IT-Betriebskonzept für das Stadtamt Bremen wurden uns Ende letzten Jahres zugestellt und im Frühjahr des Berichtszeitraums von uns bewertet. Wir haben zu den Dokumenten umfassend Stellung genommen. Derzeit werden unsere Hinweise zur Datenschutzdokumentation durch das Stadtamt Bremen aufgearbeitet. Allerdings beklagt das Stadtamt Bremen, dass aufgrund mangelnder personeller Ressourcen fraglich sei, wann eine Umsetzung des Konzeptes erfolgen kann.

Ebenso befindet sich jetzt unsere Stellungnahme zum Verfahren „AusländerDaten Verwaltungs- und InformationsSystem“ – ADVIS – (vergleiche 30. Jahresbericht, Ziffer 9.16) in Bearbeitung, mit deren Abschluss das Stadtamt Bremen aufgrund seiner Arbeitssituation zum Ende des 1. Quartals 2010 rechnet. Termine für die abschließende Beantwortung unserer Fragen und Hinweise zu Verfahren wie dem Kassensystem und der Schlüsselverwaltung, wurden uns nicht genannt. Hier wird auf umfangreiche Verfahrensänderungen verwiesen. Wir gehen davon aus, dass nach Abschluss der Arbeiten eine zeitnahe Anpassung der Datenschutzdokumente erfolgt und wir über den dann bestehenden Sachstand unterrichtet werden.

### 5.9 Kontrolle der Mobiltelefonnutzung der Verkehrsüberwacherinnen und Verkehrsüberwacher

Die Verkehrsüberwacherinnen und -überwacher des Stadtamtes sind mit Dienstmobiltelefonen für die Überwachung des ruhenden Verkehrs ausgestattet. Die Mobiltelefonnutzung wurde von ihren Vorgesetzten im Stadtamt Bremen regelmäßig kontrolliert. Dabei wurde durch eine Auswertung zum Beispiel geprüft, ob die Nutzung unbefugt privat erfolgte. Wir haben erfahren, dass Verkehrsüberwacherinnen und -überwacher mehrfach vom Amtsleiter nach privaten Beziehungen untereinander gefragt worden seien. Das Stadtamt hat auf Anfrage erklärt, nach einer Dienstanweisung sei die private Nutzung der Mobiltelefone nur in Ausnahmefällen erlaubt und die Kontrollen würden zur Überprüfung und Abrechnung privater Gespräche erfolgen.

Wir haben das Stadtamt auf die Dienstvereinbarung über die Nutzung von Telekommunikationsanlagen und Mobilfunkgeräten hingewiesen, wonach Verbindungsdaten nur zur Kostentransparenz und -zuordnung und zur Gebührenabrechnung verarbeitet werden dürfen. Nach diesen Regelungen ist die Kontrolle der Verkehrsüberwacherinnen und -überwacher nicht zulässig. Zudem ist die Kontrolle privater Beziehungen untereinander für die Betroffenen unzumutbar. Dadurch hat das Stadtamt gegen das Fernmeldegeheimnis nach dem Telekommunikationsgesetz verstoßen.

Wir haben das Stadtamt gebeten zu prüfen, ob nicht durch den Abschluss von Flatrate-Verträgen Kontrollen generell entbehrlich sind. Das Stadtamt Bremen hat uns daraufhin mitgeteilt, zukünftig die Dienstanweisung zu beachten und auf Kontrollen dieser Art zu verzichten.

### 5.10 Melderegisterauskünfte und Auskunftssperren

Die kommunalen Melderegister haben sich in den letzten Jahren mehr und mehr zu einer seitens der Wirtschaft intensiv genutzten Quelle des Anschriftenbezugs wie auch der Anschriftenaktualisierung entwickelt. Ermöglicht wird dies in erster Linie durch die sogenannte einfache Melderegisterauskunft. Hierüber können Vor- und Familiennamen, Doktorgrad und Anschriften von registerverzeichneten Einwohnerinnen und Einwohnern in Erfahrung gebracht werden. Voraussetzung der Auskunftseinholung ist lediglich, dass die Person durch Angabe einer früheren Anschrift oder sonstiger Identifizierungskriterien seitens der Anfragenden eindeutig bestimmt werden kann beziehungsweise die Anfragenden sämtliche Personen, über die sie Adressauskunft begehren, namentlich bezeichnen.

Bürgerinnen und Bürger können diese Übermittlung ihrer Daten aber dadurch verhindern oder zumindest einschränken, dass sie im Melderegister eine Auskunftssperre eintragen lassen. Gesetzlich vorgesehen ist die Möglichkeit der Eintragung einer Auskunftssperre generell zum Ausschluss von Wahlwerbung, zwecks Verhinderung der Weitergabe von Alters- und Ehejubiläen (vergleiche Ziffer 5.11 dieses Berichts) sowie gegenüber Adressbuchverlagen. Im Einzelfall müssen die Meldeämter darüber hinaus auf Antrag oder von Amts wegen eine Auskunftssperre eintragen, wenn eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen eines Betroffenen bestehen kann. Da nach den Regelungen des Melderechts generell schutzwürdige Interessen des Betroffenen durch Melderegisterauskünfte nicht beeinträchtigt werden dürfen, kann nach einer Entscheidung des Bundesverwaltungsgerichts aus dem Jahr 2006 (Urteil vom 21. Juni 2006, Aktenzeichen 6 C 5/05) im Einzelfall auch in weiteren Fallgruppen die Eintragung einer Auskunftssperre in Betracht kommen.

Entsprechende Formulare zur Eintragung von Auskunftssperren in den genannten Fällen sind im Internet unter www.bremen.de/formulare, Buchstabe „D“ beziehungsweise unter www.bremerhaven.de, Bürgerservice, Formulare, Buchstabe „E“ abrufbar und werden auch vor Ort von den Meldeämtern Bremen und Bremerhaven bereitgehalten.

### 5.11 Übermittlung und Nutzung von Einwohnermeldedaten aus Anlass von Ehe- und Altersjubiläen

Ein Bürger beklagte sich bei uns darüber, dass er aus Anlass seiner goldenen Hochzeit gemeinsam mit seiner Ehefrau Glückwünsche von einem Bremer Kreditinstitut erhalten hatte, obwohl seine Frau und er dort nicht Kunden seien und das Ehejubiläum nicht öffentlich bekannt gemacht worden sei. Auf ihre Anfrage bei der Kredit-

einrichtung, woher sie die Angaben über das Ehejubiläum erhalten habe, sei ihnen von dort mitgeteilt worden, dass die Daten von der Einwohnermeldebehörde stammten.

Begehrt jemand eine Melderegisterauskunft über Alters- oder Ehejubiläen von Einwohnerinnen und Einwohnern, so darf die Meldebehörde nach § 33 Absatz 2 Bremisches Meldegesetz (BremMeldG) die Auskunft nur dann erteilen, wenn die betroffenen Personen der Auskunftserteilung nicht widersprochen haben. Die Meldebehörde hat die betroffenen Personen auf ihr Widerspruchsrecht bei der Anmeldung und spätestens einmal jährlich durch öffentliche Bekanntmachung hinzuweisen. Da es sich bei den in § 33 BremMeldG geregelten Datenübermittlungen um besondere Fälle der Gruppenauskunft nach § 32 Absatz 3 BremMeldG handelt, bedarf es für Übermittlungen nach § 33 Absatz 2 BremMeldG darüber hinaus eines öffentlichen Interesses, dessen Vorliegen bei einer Übermittlung von Daten durch die Meldebehörde an das Kreditinstitut in diesem Fall zu verneinen gewesen wäre.

Unsere nähere Prüfung des Sachverhalts zu dieser Eingabe ergab dann jedoch, dass die Jubiläumsdaten nicht von der Meldebehörde, sondern von der Senatskanzlei an die Krediteinrichtung übermittelt worden waren. Wie wir feststellten, hat das Kreditinstitut seit vielen Jahren monatlich von der Senatskanzlei Listen mit Angaben zu Bremer Bürgerinnen und Bürgern erhalten, an deren Kenntnis es ein großes Interesse besitzt. Die Meldebehörde übermittelt an die Senatskanzlei jeden Monat auf deren Wunsch die Daten von Alters- und Ehejubilaren; bei Altersjubilaren aus Anlass des 90., 95., 100. und jedes weiteren Geburtstages, bei Ehejubilaren aus Anlass des 50., 60., 65., 70. und jedes weiteren Hochzeitstages. Übermittelt werden Familiennamen, frühere Namen, Vornamen, Geschlecht, akademische Grade, die Anschrift sowie der Tag der Geburt beziehungsweise der Tag der Eheschließung auf der Basis des § 6 der Meldedatenübermittlungsverordnung (MeldDÜVO). Von der Senatskanzlei wurden die vorstehenden Listen auch an eine Bremer Wohnungsbaugesellschaft versandt. Da es keine Rechtsgrundlage für die Datenübermittlungen von ihr an die genannten Unternehmen gibt, sagte die Senatskanzlei auf unsere Aufforderung hin zu, die Listen künftig nicht mehr zu übersenden.

Komplette Listen mit den Daten aller der Senatskanzlei mitgeteilten Alters- und Ehejubilare sind von dieser bislang auch an mehrere Ortsämter in Bremen versandt worden. Im Hinblick auf die räumlich begrenzten Zuständigkeitsbereiche der Ortsämter haben wir die Übermittlung sämtlicher Daten der Senatskanzlei mitgeteilten Jubilare zunächst kritisiert und gebeten, die Inhalte der Listen zu begrenzen. Um eine weitergehende datenschutzrechtliche Bewertung vornehmen zu können, stellt sich außerdem die Frage, in welcher Rechtsbeziehung die beteiligten Ortsämter die Aufgabe der Ehrung von Ehe- und Altersjubilaren wahrnehmen. Eine abschließende Klärung mit der Senatskanzlei steht dazu noch aus.

### 5.12 Einrichtung eines automatisierten Direktzugriffs auf Melderegisterdaten für Kommunalbehörden in Bremen und Bremerhaven ohne gesetzliche Grundlage

Nach wie vor nicht beigelegt werden konnte der bereits im vergangenen Tätigkeitsbericht (vergleiche 31. Jahresbericht, Ziffer 9.3) dargelegte Konflikt um die notwendigen rechtlichen Grundlagen eines automatisierten Direktzugriffs von Gemeindebehörden auf die Melderegisterdaten der jeweiligen kommunalen Meldebehörde in Bremen beziehungsweise in Bremerhaven.

Nach § 30 Absatz 4 Bremisches Meldegesetz (BremMeldG) bedürfen regelmäßige Datenübermittlungen – auch in der Form eines automatisierten Direktzugriffs – von Melderegisterdaten an andere öffentliche Stellen einer expliziten rechtlichen Grundlage, etwa in einer Rechtsverordnung, in der Anlass, Zweck, Datenübermittlungsumfang und empfangende Stelle klar bestimmt sind. Mit dieser Regelung soll nicht zuletzt sichergestellt werden, dass Datenübermittlungen für Bürgerinnen und Bürger transparent beziehungsweise jederzeit nachvollziehbar sind. Die Bürgerinnen und Bürger sollen nämlich grundsätzlich wissen können, wer was bei welcher Gelegenheit zu welchem Zweck über sie weiß. Anfang 2007 wies jedoch der Senator für Inneres und Sport die nachgeordneten Meldebehörden in einem Auslegungserlass darauf hin, dass seiner Auffassung nach innerhalb der Stadtgemeinde Bremen Meldedaten von der Meldebehörde in Bremen an sonstige öffentliche Stellen der Stadtgemeinde Bremen weitergegeben werden dürften, ohne dass es einer speziellen gesetzlichen Regelung dieser Datenübermittlungen bedürfe. Entsprechen-

des gelte für Bremerhaven. Zur Begründung wurde auf die vermeintlich gegenüber Absatz 4 spezielle Regelung des § 30 Absatz 5 BremMeldG verwiesen.

Wir hatten dem Senator für Inneres und Sport daraufhin mitgeteilt, dass wir diesen Erlass als eindeutig rechtswidrig und damit nichtig erachten, und ihn darum gebeten, aus Gründen der Rechtssicherheit den Erlass aufzuheben. Ausführlich hatten wir unsere Auffassung begründet. Unter anderem hatten wir darauf hingewiesen, dass regelmäßige Datenübermittlungen, insbesondere in der Form eines automatisierten Abrufverfahrens, mit besonderen Gefährdungen des Persönlichkeitsrechts Betroffener verbunden sind. Automatisierte Datenweitergaben auf Abruf zwischen Gemeindebehörden unterscheiden sich hinsichtlich dieser Gefährdungslage für das Persönlichkeitsrecht nicht von automatisierten regelmäßigen Datenübermittlungen zwischen Behörden unterschiedlicher Verwaltungsträger. Schon aus diesem Grund können für regelmäßige Datenweitergaben zwischen Gemeindebehörden keine geringeren Anforderungen gelten, als sie nach § 30 Absatz 4 BremMeldG an Meldedatenübermittlungen etwa an Landesbehörden gestellt werden. Auch die öffentliche Gemeindeverwaltung mit ihren zahlreichen unterschiedlichen Fachbehörden stellt keine Informationseinheit dar, in der personenbezogene Daten ohne Wissen der Betroffenen frei zur jeweiligen Aufgabenerfüllung ausgetauscht werden können. Vielmehr gilt auch hier von Verfassungs-wegen das sogenannte Gebot der informationellen Gewaltenteilung.

Dass Datenweitergaben innerhalb einer Verwaltungseinheit in Form eines automatisierten Abrufs einer gesonderten – verfassungsgemäßen – Rechtsgrundlage, wie sie auch § 30 Absatz 4 BremMeldG fordert, bedürfen, ergibt sich letztlich auch eindeutig aus der Vorschrift des § 14 Absatz 4 Bremisches Datenschutzgesetz (BremDSG). § 14 Absatz 4 BremDSG schreibt nämlich unmissverständlich vor, dass es für die Einrichtung automatisierter Abrufverfahren innerhalb einer öffentlichen Stelle unter der Voraussetzung, dass die übermittelnde und die abrufende Einheit der öffentlichen Stelle unterschiedliche Aufgaben wahrnehmen, einer Rechtsverordnung bedarf.

Auch der Senator für Justiz und Verfassung kam in einer ausführlich begründeten Stellungnahme zu der Ansicht, dass unsere Rechtsauffassung zutreffend sei. Nach einem Gespräch mit dem Senator für Inneres und Sport zog der Senator für Justiz und Verfassung seine Bedenken ohne nähere Begründung jedoch zurück.

Der Senator für Inneres und Sport beharrt weiterhin auf seiner Auffassung und weigerte sich bis dato, den Erlass aufzuheben. Wir werden die Sache weiterverfolgen.

### 5.13 Gekennzeichnete Wahlzettel bei der Europawahl

Anlässlich der Europawahl 2009 wandten sich einige Wählerinnen und Wähler an uns, weil sie sich darüber wunderten, dass ihre Briefwahlzettel mit den Merkmalen Wahlbezirk, Geschlecht und Geburtsjahresgruppe gekennzeichnet waren. Sie befürchteten eine Gefährdung des Wahlgeheimnisses.

Die Kennzeichnung der Wahlzettel diente der Durchführung einer repräsentativen statistischen Wahluntersuchung. Gesetzliche Grundlage hierfür ist das Wahlstatistikgesetz in Verbindung mit dem Bundesstatistikgesetz.

Der Gesetzgeber hat in diesen Gesetzen Vorkehrungen getroffen, die eine Gefährdung des Wahlgeheimnisses ausschließen. So kommt für die Statistik nur ein Briefwahlbezirk in Betracht, der mindestens 400 Wählerinnen und Wähler umfasst. Es erfolgt keine Erfassung nach einzelnen Geburtsjahrgängen, sondern die Geburtsjahrgänge werden zu Gruppen zusammengefasst, sodass das individuelle Geburtsjahr der Wählerin oder des Wählers nicht erkennbar und nicht ermittelbar ist. Der Wahlbezirk wird nur als sogenanntes Hilfsmerkmal (ein Merkmal, das letztlich nur der ordnungsgemäßen Abwicklung der Statistik in den Statistikämtern dient, nicht aber für die Statistik selbst Verwendung findet) erfasst. Hilfsmerkmale sind nach Überprüfung der Schlüssigkeit und Vollständigkeit der erhobenen Merkmale – hier: Geschlecht, Geburtsjahresgruppe, Stimmabgabe – zu löschen. Die gekennzeichneten Stimmzettel werden ungeöffnet zur Auswertung an die statistischen Ämter geleitet, für diese Ämter gelten strikte Geheimhaltungspflichten. Darüber hinaus dürfen Wählerverzeichnis und gekennzeichnete Stimmzettel nicht zusammengeführt werden. Durch diese gesetzlichen Vorgaben dürfte in ausreichendem Maße sichergestellt sein, dass die individuelle Stimmabgabe nicht einer bestimmten wählenden Person zugeordnet werden kann.

Durch Erläuterung dieser gesetzlichen Sicherungsmechanismen konnten wir die Befürchtungen der anfragenden Wählerinnen und Wähler zerstreuen.

## 6. Justiz

### 6.1 Verwendung von Privatadressen von Gerichtsvollzieherinnen und Gerichtsvollziehern durch die Polizei

Ein Gerichtsvollzieher beschwerte sich bei uns über eine polizeiliche Ladung, welche an seine private Anschrift gesandt worden war. Er sollte Stellung zu einer Anzeige gegen ihn wegen Hausfriedensbruchs nehmen. Die Tat sollte er im Rahmen seiner dienstlichen Vollstreckungstätigkeit begangen haben. Anzeigenerstatter war ein Schuldner, für den der Gerichtsvollzieher zuständig war. In der Anzeige war die Dienstanschrift des Gerichtsvollziehers angegeben. Bei der Polizei erfolgte dann routinemäßig die Ermittlung der aktuellen Anschrift über eine automatisierte Abfrage der Einwohnermeldedaten, sogenannte Meso-Abfrage gemäß § 5 Absatz 5 Bremische Meldedatenübermittlungsverordnung (BremMeldDÜVO). Die Meso-Abfrage ergab eine von der in der Anzeige abweichende Anschrift, die die Polizei Bremen dafür verwendete, dem Gerichtsvollzieher Gelegenheit zur Stellungnahme zur Sache einzuräumen. Wie sich im Nachhinein herausstellte, handelte es sich um die Privatadresse des Gerichtsvollziehers.

Die Privatanschrift von Gerichtsvollzieherinnen und Gerichtsvollziehern ist im Hinblick auf die Abwendung von Gefahren für das private und familiäre Umfeld besonders schützenswert. Die Problematik wurde mit der Polizei Bremen erörtert. Wir vereinbarten, dass – sofern eine Gerichtsvollzieherin oder ein Gerichtsvollzieher dienstlich tätig geworden ist – davon abzusehen ist, die Privatanschrift in die Ermittlungsakte beziehungsweise in die polizeilichen Ermittlungssysteme aufzunehmen. Da die Polizei über eine Meldeabfrage lediglich die private Anschrift, nicht jedoch die Dienstanschrift ermitteln kann, wird in der Regel der Postweg über die Gerichtsvollzieherverteilerstelle genutzt werden. Diese Vereinbarung teilten wir den im Land Bremen tätigten Gerichtsvollzieherinnen und Gerichtsvollziehern in einem Rundschreiben mit.

Im Übrigen wiesen wir die Gerichtsvollzieherinnen und Gerichtsvollzieher darauf hin, dass sie eine Auskunftssperre beim Stadtamt, Meldebehörde, veranlassen können. Bei einer dann stattfindenden Meso-Abfrage durch die Polizei ist eine automatische Datenübermittlung gemäß § 20 Absatz 2 BremMeldDÜVO ausgeschlossen. Hier wird allein durch den Hinweis, dass eine Meso-Abfrage nicht möglich ist, die Polizei sensibilisiert.

### 6.2 Erstellung einer Orientierungshilfe für Notariate

Mitte dieses Jahres trat die Notaraufsicht beim Landgericht an uns heran und bat uns um datenschutzrechtliche Unterstützung im Rahmen ihrer Aufsichtstätigkeit. Aufgrund bestehender gesetzlicher Geheimhaltungspflichten und der Sensibilität der im Notariat zu verarbeitenden Daten, zum Beispiel in Eheverträgen oder Testamenten, muss dem Datenschutz bei Notarinnen und Notaren ein hoher Stellenwert beigemessen werden. Bereits im Jahr 2004 hatten wir zufällig ausgewählte Notarinnen und Notare datenschutzrechtlich geprüft und, aufgrund der damals festgestellten Mängel, diverse datenschutzrechtliche Anforderungen an den Datenschutz im Notariat formuliert und diese der Notarkammer mitgeteilt. In diesem Zusammenhang wurde auch ein behördlicher Datenschutzbeauftragter bei der Notarkammer bestellt, welcher für alle Notarinnen und Notare Ansprechpartner in Sachen Datenschutz ist.

Aufgrund der guten Resonanz auf unsere Orientierungshilfe „Datenschutz bei Gerichtsvollziehern“ im letzten Jahr boten wir auch der Notaraufsicht an, für den Datenschutz bei Notarinnen und Notaren eine Orientierungshilfe herauszugeben. Diese haben wir Ende dieses Jahres der Notaraufsicht mit der Bitte, diese an die Notariate weiterzuleiten, übersandt. Die Orientierungshilfe geht sowohl auf die herkömmliche Datenverarbeitung in Papierakten als auch auf die elektronische Datenverarbeitung ein. Schwerpunkt ist allerdings die elektronische Datenverarbeitung, da besonders dieser Bereich erhebliche Gefahren in sich birgt. Hierbei wird die Konfigurationen von PC, Datensicherung, die Nutzung des Internets, WLAN, mobile Endgeräte, Fernwartung und die Entsorgung von Altgeräten und Daten-

trägern behandelt. Die Orientierungshilfe ist auch auf unserer Homepage unter www.datenschutz.bremen.de/recht herunterzuladen.

### 6.3 Beratung des Bremischen Untersuchungshaftvollzugsgesetzes

Mit der ersten Stufe der Föderalismusreform ist die Gesetzgebungskompetenz für den Strafvollzug auf die Länder übergegangen. Zuerst wurde 2007 das Bremische Jugendstrafvollzugsgesetz (BremJStVollzG) verabschiedet, daran anschließend wurde das Bremische Untersuchungshaftvollzugsgesetz (BremUVollzG) in Angriff genommen. Von der Mehrzahl der Landesjustizverwaltungen wurde ein Musterentwurf erarbeitet. Auf dieser Basis erarbeitete der Senator für Justiz und Verfassung unter Einbeziehung der Diskussion über das Bremische Jugendstrafvollzugsgesetz einen Entwurf, den er uns zur Stellungnahme übersandte. Bedauerlicherweise fanden die in unserer Stellungnahme geäußerten datenschutzrechtlichen Bedenken bezüglich der Erfassung von biometrischen Merkmalen, der fehlenden Normenklarheit in der Regelung zur Zentralen Datei und des geringen Schutzes der Kommunikation mit Berufsgeheimnisträgern, die nicht Verteidiger sind, zum Beispiel Schwangerschafts- und Drogenberatung, keine Berücksichtigung. Es wurden aber auch viele unserer Anregungen vom Senator für Justiz und Verfassung übernommen.

So sah der Entwurf vor, dass bei Zugangsgesprächen andere Gefangene in der Regel nicht zugegen sein dürfen. Da für Untersuchungsgefangene eine Unschuldsvermutung gilt, sind ihre personenbezogenen Daten, die sie insbesondere im Zugangsgespräch angeben müssen, als besonders sensible Daten einzustufen, sodass eine Kenntnisnahme durch Dritte – also nicht Anstaltspersonal in deren Aufgabenerfüllung – ausgeschlossen sein sollte. Aufgrund unserer Anregung wurden die Worte in der Regel gestrichen, sodass gewährleistet ist, dass Dritte bei den Zugangsgesprächen nicht anwesend sind.

Eine Regelung zur Gesundheitsvorsorge sah vor, dass Angehörige zu benachrichtigen sind, wenn Untersuchungsgefangene schwer erkranken. Dies wurde in der Begründung als humanitäre Verpflichtung der Anstalt bezeichnet. In der Regel wird die Verfahrensweise auch dem Interesse der Untersuchungsgefangenen entsprechen. Die Betroffenen sollten jedoch das Recht haben, selbst über die Übermittlung an ihre Angehörigen zu bestimmen. Der Senator für Justiz und Verfassung hat diesbezüglich unsere Anregung umgesetzt. Nunmehr ist grundsätzlich die Einwilligung der Untersuchungsgefangenen erforderlich. Wenn die Einwilligung nicht erlangt werden kann, erfolgt die Benachrichtigung, wenn die Untersuchungsgefangenen einer Benachrichtigung nicht widersprochen haben und keine sonstigen Anhaltspunkte dafür bestehen, dass eine Benachrichtigung nicht angebracht ist.

Hinsichtlich der Überwachung von Besuchen wurde klargestellt, dass eine Aufzeichnung nicht stattfindet, da es auch vom Senator für Justiz und Verfassung für ausreichend erachtet wird, das Geschehen live zu beobachten und gegebenenfalls einzuschreiten.

Andere Anregungen und Bedenken, die wir bereits in der Beratung des Bremischen Jugendstrafvollzugsgesetzes geäußert haben, fanden auch im Rahmen dieses Entwurfs keine Berücksichtigung. Der Senator für Justiz und Verfassung hat uns aber zugesagt, dass die Bedenken bei der Novellierung des Strafvollzugsgesetzes 2010/2011 erneut aufgegriffen werden sollen. Insoweit wären dann das Jugendstrafvollzugsgesetz und das Untersuchungshaftvollzugsgesetz anzupassen.

### 6.4 Bewährungshelferinnen und Bewährungshelfern werden Berufsgeheimnisse anvertraut

Wie wir bereits im letzten Jahresbericht thematisiert haben (vergleiche 31. Jahresbericht, Ziffer 10.2) besteht zwischen dem Senator für Justiz und Verfassung und der Landesbeauftragten für Datenschutz und Informationsfreiheit Uneinigkeit darüber, ob Bewährungshelferinnen und Bewährungshelfern Berufsgeheimnisse anvertraut werden.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit vertritt die Auffassung, dass Bewährungshelferinnen und Bewährungshelfer gemäß § 203 Absatz 1 Nummer 5 Strafgesetzbuch (StGB) uneingeschränkt als Berufsgeheimnisträger zu qualifizieren sind. Die Vorschrift legt fest, dass Sozialpädagoginnen und Sozialpädagogen Berufsgeheimnisträger sind. Bewährungshelferinnen und Bewährungs-

helfer gehören zu dieser Berufsgruppe. Die Formulierung der gesetzlichen Regelung ist eindeutig in ihrer Formulierung und lässt keine anderweitigen Interpretationen zu. Der Gesetzgeber hat für die Bewährungshilfe bewusst nur eine einzige ausdrückliche Datenübermittlungsvorschrift geschaffen, nämlich in § 56 d Absatz 3 Satz 3 StGB eine Berichtspflicht an das Gericht. Durch anderweitiges Offenbaren würde sich die Bewährungshelferin beziehungsweise der Bewährungshelfer strafbar machen. Allerdings kann in Ausnahmefällen eine Offenbarung gerechtfertigt sein, wenn die Betroffenen eingewilligt haben oder die Voraussetzungen des rechtfertigenden Notstandes, § 34 StGB, erfüllt sind. Die Voraussetzungen wären zum Beispiel erfüllt, wenn eine gegenwärtige, nicht anders abwendbare Gefahr für Leib oder Leben für andere bestünde. Die Rechtsauffassung der Landesbeauftragten für Datenschutz und Informationsfreiheit Bremens wird vom Arbeitskreis Justiz der Konferenz der Datenschutzbeauftragten des Bundes und der Länder geteilt.

Der Senator für Justiz und Verfassung geht davon aus, dass die Bewährungshelferinnen und Bewährungshelfer keine Berufsgeheimnisträger sind und sie lediglich der allgemeinen Pflicht zur Amtsverschwiegenheit unterliegen. Das hätte zur Folge, dass die allgemeinen Übermittlungsvorschriften des Bremischen Datenschutzgesetzes (BremDSG) anwendbar wären. Hiernach wäre zum Beispiel auch eine Datenweitergabe an andere öffentliche Stellen zur Verfolgung von Ordnungswidrigkeiten zulässig. Eine solche Datenübermittlung stünde im eklatanten Widerspruch zum Vertrauensverhältnis zwischen Bewährungshelferinnen und Bewährungshelfern und den Klientinnen und Klienten. Weiterhin wird vom Senator für Justiz und Verfassung vorgetragen, dass die Problematik eher theoretischer Natur sei. Dem steht jedoch entgegen, dass sich die Bewährungshilfe 2008 mit genau dieser Fragestellung an uns gewandt hatte, weil eine erheblichen Rechtsunsicherheit bestand.

Aufgrund des bestehenden Dissenses wurde das Problem im Herbst auch im Parlamentsausschuss für Informations- und Kommunikationstechnologie und Medienangelegenheiten der Bremischen Bürgerschaft, Medienausschuss, behandelt. Dort berichtete der Senator für Justiz und Verfassung, dass der Senat seine Rechtsauffassung gegenüber den Bewährungshelferinnen und Bewährungshelfern in einem Brief dargelegt habe. Zudem teile auch die Generalstaatsanwältin die Auffassung des Justizressorts, sodass eine Bewährungshelferin beziehungsweise ein Bewährungshelfer keine Strafverfolgung zu erwarten hätte.

Schließlich wurde die Problematik auch auf der Justizministerkonferenz erörtert. In einem Beschluss bitten die Justizministerinnen und Justizminister den Strafrechtsausschuss um Prüfung, ob die Schaffung ergänzender Regelungen für den Austausch personenbezogener Daten unter anderem zwischen Bewährungshilfe, Staatsanwaltschaft, Polizei und den Einrichtungen des Justiz- und Maßregelvollzugs sinnvoll ist. Auch anhand dieses Beschlusses zeigt sich, dass die bestehende Rechtslage geändert werden müsste, um weitergehende Übermittlungsbefugnisse aufseiten der Bewährungshilfe zu erhalten. Zu diesem Ergebnis kommt übrigens auch eine beim Justizministerium Brandenburg eingerichtete Arbeitsgruppe. In ihrer Handreichung heißt es: „Im Interesse der staatlich geprüften Bewährungshelfer sollte derzeit allerdings von der strengeren Geheimhaltungspflicht nach § 203 Absatz 1 Nummer 5 StGB ausgegangen werden“.

Ob tatsächlich die Schaffung einer Rechtgrundlage der richtige Weg wäre, ist zu bezweifeln, da es dadurch bei der Bewährungshilfe zu einer Aufgabenverschiebung käme, bei der das Vertrauensverhältnis zwischen der Bewährungshilfe und ihren Klientinnen und Klienten nur noch sehr rudimentär bestehen würde. Allerdings ist der derzeitige Zustand im Sinne der Rechtssicherheit nicht akzeptabel.

## 7. Gesundheit und Soziales

### 7.1 Beschäftigtenscreening als Unterschlagungsprüfung ohne Anlass

Der Eigenbetrieb KiTa Bremen hatte einen Wirtschaftsprüfer beauftragt, eine Unterschlagungsprüfung vorzunehmen mit dem Ziel, sogenannte dolose Handlungen (vorsätzlich begangene strafbare Handlungen) im Bereich der Finanzbuchhaltung aufzuklären, ohne dass hierfür ein konkreter Anlass bestand. Dazu übermittelte KiTa Bremen dem Wirtschaftsprüfer die Personalnummern, Namen, Privatanschriften und -telefonnummern sowie die Bankverbindungsdaten aller 1.500 Beschäftigten der KiTa Bremen und die Kontodaten der Lieferanten beziehungsweise Kreditoren. Der beauftragte Wirtschaftsprüfer glich die Beschäftigtendaten mit der Auswertungs-

software IDEA ab (sogenanntes Screening, das heißt, Rasterung, Selektion und so weiter). Die Auswertung erbrachte eine Übereinstimmung in 319 Fällen. Dabei stellte sich heraus, dass in all diesen Fällen rechtmäßig Lieferantenkonten für Beschäftigte der Kindertagesstätten eingerichtet worden waren, um ihnen Auslagen für pädagogisches Material und für die Verpflegung der Kinder bargeldlos zu ersetzen.

Über das Screening wurden nach Angaben von KiTa Bremen die ungefähr zehn Beschäftigten der Buchhaltung vor und nach der Prüfung unterrichtet. Eine Unterrichtung der übrigen Beschäftigten unterblieb.

Dieses Screening verstieß gegen das Bremische Datenschutzgesetz (BremDSG) und das Bremische Beamtengesetz (BBG). Danach ist eine Datenverarbeitung über Beschäftigte und Lieferanten nur zulässig, soweit sie zur Durchführung organisatorischer Maßnahmen und zur rechtmäßigen Aufgabenerfüllung erforderlich ist und dadurch keine schutzwürdigen Belange der Beschäftigten beeinträchtigt werden. Diese Vorschriften sind unter Beachtung der Rechtsprechung des Bundesverfassungsgerichts und des Bundesarbeitsgerichts sowie der Kriterien zur Bestimmung der Verhältnismäßigkeit einer Überwachungsmaßnahme, die das Bundesverfassungsgericht in seiner Entscheidung zur Rasterfahndung entwickelt hat, auch auf die Arbeitnehmerkontrolle anzuwenden.

Das Bundesverfassungsgericht hatte festgestellt, dass die Rasterfahndung einen erheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt und konkrete Gründe für die Durchführung einer Rasterfahndung erforderlich sind. Nach diesen Maßstäben verlangt das Bundesarbeitsgericht bei Überwachungen von Beschäftigten eine „Verhältnismäßigkeit im engeren Sinne“. Dazu bedarf es einer Gesamtabwägung der Intensität des Eingriffs und des Gewichts der ihn rechtfertigenden Gründe. Für die Schwere des Eingriffs ist insbesondere von Bedeutung, wie viele Personen wie intensiv den Beeinträchtigungen ausgesetzt sind, welche Nachteile den Betroffenen aus der Überwachungsmaßnahme drohen oder von ihnen nicht ohne Grund befürchtet werden müssen. Ferner sind in die Abwägung die Dauer und die Art der Maßnahme und die Frage einzubeziehen, ob die Betroffenen einen ihnen zurechenbaren Anlass für die Datenerhebung geschaffen haben – etwa durch eine Rechtsverletzung –, oder ob dies anlasslos erfolgt. Die Heimlichkeit einer in Grundrechte eingreifenden Ermittlungsmaßnahme erhöht das Gewicht der Freiheitsbeeinträchtigung. Den Betroffenen wird hierdurch vorzeitiger Rechtsschutz faktisch verwehrt und nachträglicher Rechtsschutz erschwert. Demzufolge haben wir folgende Mängel festgestellt:

— Im Rahmen der Vorabkontrolle hätte untersucht werden müssen, ob technische und organisatorische Maßnahmen getroffen worden sind, die strafrechtliches Verhalten angemessen verhindert, und gegebenenfalls, wie diese Maßnahmen verbessert werden können, zum Beispiel Einsatz des Vier-Augen-Prinzips bei der Anlegung von Kreditoren, regelmäßiger Passwortwechsel durch die Zugriffsberechtigten auf das Datenverarbeitungssystem.

— Das Beschäftigtenscreening hätte sich – wenn überhaupt – allenfalls auf die Personen begrenzen müssen, die befugt sind, Kreditoren einzurichten, also nur die ungefähr zehn Beschäftigten des Referats „Finanz- und Rechnungswesen“ der KiTa Bremen.

— Darüber hinaus sind alle 1.500 Beschäftigten der KiTa Bremen durch die Unterschlagungsprüfung zur Aufdeckung vorsätzlich begangener Straftaten ohne konkreten Anlass einem Generalverdacht ausgesetzt gewesen, sodass dadurch ihre schutzwürdigen Belange erheblich beeinträchtigt worden sind.

Des Weiteren sollten vor derartigen Überwachungsmaßnahmen insbesondere folgende Voraussetzungen im Rahmen einer Vorabkontrolle geklärt werden:

1. Es ist zu prüfen, ob es anstelle eines Screeningverfahrens ein milderes Mittel zur Erreichung des Zwecks gibt, das weniger oder gar nicht in das Persönlichkeitsrecht der Betroffenen eingreift. Ebenfalls ist zu klären, ob das Screening pseudonymisiert durchgeführt werden kann. Dies ist zu dokumentieren.

2. Vor Beginn der Maßnahme und während ihres Verlaufs sind die oder der behördliche Datenschutzbeauftragte und der Personalrat beziehungsweise der Betriebsrat zu beteiligen.

3. Beschäftigte, bei denen durch das Screening Auffälligkeiten festgestellt werden, befinden sich im Vorfeld des Verdachts. Dies kann für sie zu verschiede-

nen Nachteilen führen. Deshalb sind Verdachtsfälle unverzüglich aufzuarbeiten. Dabei ist ein Verfahren anzuwenden, das die schutzwürdigen Belange der Betroffenen wahrt. Beispielsweise sollte festgelegt werden, dass die Sichtung der Treffen und die Festlegung weiterer Maßnahmen unter Beteiligung der Personalvertretung und des beziehungsweise der behördlichen Datenschutzbeauftragten erfolgen. In Anbetracht der hohen Sensibilität der Daten ist für den Schutz vor unbefugten Zugriffen und zweckwidriger Verwendung zu sorgen.

4. Schutzwürdige Belange der Betroffenen werden dann beeinträchtigt, wenn der Arbeitgeber beziehungsweise der Dienstherr bei einer Überprüfung nicht die größtmögliche Transparenz sicherstellt, soweit hierdurch nicht der festgelegte Zweck gefährdet würde. Eine vorherige Unterrichtung über die beabsichtigte Überprüfung ist dabei einer späteren Benachrichtigung vorzuziehen. Insbesondere sind aber die Personen zu unterrichten beziehungsweise zu benachrichtigen, die sich im Vorfeld des Verdachts befinden oder befanden.

5. Es ist sicherzustellen, dass die verantwortliche Stelle die personenbezogenen Daten der Beschäftigten, die sich im Vorfeld des Verdachts befinden, unverzüglich löscht, falls sich der Verdacht nicht bestätigt.

6. Bei der Einschaltung von Drittunternehmen ist zu vermeiden, dass Personaldaten übermittelt werden, und es ist zu prüfen, ob die Übermittlung von Pseudonymen ausreicht. Außerdem sind die Zwecke genau schriftlich festzulegen, nach denen Beschäftigtendaten verarbeitet und genutzt werden dürfen, sowie sicherzustellen, dass nach Beendigung des Auftrags beim Drittunternehmen sämtliche übergebenen personenbezogenen Daten unverzüglich gelöscht werden.

7. Nach jedem Screening muss eine Evaluation erfolgen. Hierdurch soll vermieden werden, dass Screeningverfahren, die das informationelle Selbstbestimmungsrecht der Beschäftigten tangieren, durchgeführt werden, obwohl diese zu keinen beziehungsweise zu vernachlässigbaren Ergebnissen führen.

Wir haben von der KiTa Bremen verlangt, für ein datenschutzkonformes Screening zukünftig die vorgenannten Maßnahmen durchzuführen und die noch nicht informierten Beschäftigten über das durchgeführte Screening zu benachrichtigen. Der Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales als Aufsichtsbehörde über die KiTa Bremen haben wir vorgeschlagen, die übrigen öffentlichen Stellen des Landes und der Stadtgemeinden Bremen und Bremerhaven über die Voraussetzungen zur Durchführung eines Screenings zu informieren. Dies ist erfolgt. Der Wirtschaftsprüfer ist aufgefordert worden, bei weiteren Screenings ebenfalls die vorgenannten Vorgaben zu beachten.

Alle Beteiligten haben die Einhaltung der Vorgaben zukünftig zu beachten. Das Ressort hat zudem erklärt, die Problematik in die Runde Innenrevisionen der bremischen Verwaltung einzubringen.

### 7.2 „Stopp der Jugendgewalt" – Projekt „Voll im Blick"

Im März bat uns das Landesinstitut für Schule (LIS) um Prüfung der Konzeptunterlagen des Projektes „Voll im Blick" aus dem Handlungskonzept „Stopp der Jugendgewalt" (vergleiche dazu auch Ziffer 5.2 dieses Berichts). Mit diesem Projekt sollte ein Frühwarnsystem bei Alkoholmissbrauch von Kindern und Jugendlichen geschaffen werden. Geplant war, dass bei bekannt werden von Alkoholmissbrauch bei Kindern und Jugendlichen ohne Einwilligung der Betroffenen von Polizei, Krankenhäusern und Schulen Meldungen an eine zentrale Meldestelle im Amt für Soziale Dienste (AfSD), Abteilung Junge Menschen und Familie, erfolgen. Von dort sollte die Einleitung von Jugend- und Familienhilfemaßnahmen koordiniert und kontrolliert werden, eine Weiterleitung der Betroffenen an Erziehungsberatungsstellen, den Kinder- und Jugendpsychiatrischen Dienst und das Zentrum für schülerbezogene Beratung stattfinden sowie eine Evaluation durchgeführt werden. Unsere Prüfung ergab, dass es für die in diesem Konzept vorgesehenen Datenübermittlungen überwiegend keine Rechtsgrundlagen gab beziehungsweise die Voraussetzungen der bestehenden Rechtsgrundlagen nicht erfüllt waren. Wir begleiteten die Umstellung des Projektes der Datenübermittlungen auf Einwilligungsbasis durch das LIS, einschließlich der Erstellung der verwendeten Formulare für Schweigepflichtentbindungserklärungen und Meldungen. Dabei wurden Datenübermittlungen auf das erforderliche Maß reduziert. Es dürfen keine Daten von Dritten übermittelt wer-

den. Daneben müssen die Datenübermittlungen den Betroffenen gegenüber transparent gemacht werden. Die Meldungen der Krankenhäuser an das AfSD erfolgen nur bei Vorliegen einer Schweigepflichtentbindungserklärung der Betroffenen. Die Meldungen der Polizei ohne Einwilligung der Betroffenen erfolgen nur – wie gesetzlich vorgesehen – im Einzelfall bei Vorliegen einer erheblichen sozialen Notlage, grundsätzlich nach einem persönlichen Gespräch mit den Erziehungsberechtigten. Auch die weiteren Datenübermittlungen vom Amt für Soziale Dienste an Beratungsstellen finden nur mit Einwilligung der Betroffenen statt. Zudem wurde sichergestellt, dass für Datenübermittlungen ein sicherer Transportweg gewählt wird. Die Evaluation wird nur anhand von anonymisierten Datensätzen durchgeführt.

### 7.3 BAgIS / ARGE Job-Center Bremerhaven

Auch im Berichtsjahr waren wieder zahlreiche Eingaben von Hilfeempfängerinnen und -empfängern zu Datenschutzverstößen der Bremer Arbeitsgemeinschaft für Integration und Soziales (BAgIS) beziehungsweise Arbeitsgemeinschaft (ARGE) Job-Center Bremerhaven zu verzeichnen. Im Zusammenhang mit Presseberichten zu Datenschutzproblemen bei der BAgIS hatte es im Juli eine Kleine Anfrage der Fraktion Bündnis 90/Die Grünen zu diesem Thema gegeben. In der Antwort des Senats werden die Gründe für wiederholte Verstöße gegen den Sozialdatenschutz in der personellen Ausstattung, der hohen Fluktuation des Personals, dem Arbeitsvolumen, den Rückständen in der Bearbeitung von Verfahren sowie in der ungeklärten Zukunft der ARGEn verortet. Es wird versichert, dass die Einhaltung des Datenschutzes für die Grundsicherungsträger einen hohen Stellenwert habe und dass die BAgIS ihre Mitarbeiterinnen und Mitarbeiter regelmäßig auf allen Hierarchieebenen im Datenschutz schule. Vertrauliche Hinweise von Mitarbeiterinnen und Mitarbeitern der BAgIS lassen jedoch Zweifel daran aufkommen, dass die Sachbearbeiterinnen und Sachbearbeiter Schulungen im Datenschutz erhalten haben. Zumindest aber hat die Geschäftsleitung mit einen Brief an alle dort Beschäftigten reagiert, in dem sie die Bedeutung des Sozialdatenschutzes betont und sie bittet, mit den Sozialdaten der Betroffenen sensibel, verantwortungsvoll und gewissenhaft umzugehen. In der Antwort des Senats wurde versichert, dass geprüft werde, wie die Vertraulichkeit von Gesprächen mit Hilfeempfängerinnen und Hilfeempfängern unter den gegebenen räumlichen Verhältnissen verbessert werden könne. Auf unsere Nachfrage nach umgesetzten Verbesserungen haben wir von der BAgIS erfahren, dass ab Februar 2010 Schulungen der Mitarbeiterinnen und Mitarbeiter im Datenschutz durchgeführt werden sollen.

Die im Folgenden geschilderten Fälle zeigen auf, dass noch Verbesserungen nötig sind.

**Mangelnde Vertraulichkeit in Gesprächssituationen**

Anlass der Kritik war häufig wieder die mangelnde Vertraulichkeit der äußerst sensiblen Gespräche in den Büros, in denen mehrere Sachbearbeiterinnen oder Sachbearbeiter gleichzeitig Gespräche mit Hilfeempfängerinnen oder Hilfeempfängern führen. Beispielsweise sind in der BAgIS Ost II die Schreibtische aufgrund der räumlichen Enge nur notdürftig optisch durch Stellwände voneinander abgeschirmt. Da wir mit der BAgIS vereinbart hatten, dass in ihren Räumen für Kundinnen und Kunden gut sichtbar Schilder mit dem Hinweis auf die Möglichkeit einer vertraulichen Einzelberatung aufgestellt werden, wunderte uns, dass Betroffene berichteten, in der BAgIS Ost II kein entsprechendes Schild gesehen zu haben. Die BAgIS teilte dazu mit, dass die Schilder durch Verschleiß und andere Umstände zwischenzeitlich wieder entfernt worden waren und versicherte, diese nun wieder aufzuhängen.

Wir forderten die BAgIS auf, zusätzlich in allen Geschäftsstellen mit Publikumsverkehr in mehrfach besetzten Büros an den Beratungstischen einen Sichtschutz durch Stellwände einzurichten. Da bereits die durch die Beratung von mehreren Hilfeempfängerinnen und Hilfeempfängern in einem Raum geschaffene Möglichkeit zum Mithören der Gespräche durch unbefugte Dritte einen Verstoß gegen die Pflicht zur Wahrung des Sozialgeheimnisses darstellt, halten wir diese Maßnahmen für unbedingt erforderlich, um wenigstens ein Mindestmaß an Vertraulichkeit sicherzustellen. Dazu teilte die BAgIS mit, dass das Aufstellen zusätzlicher Stellwände aus Platzgründen aus ihrer Sicht nicht möglich sei. Diesen Einwand halten wir für unbegründet, da für das Aufstellen einer wenige Zentimeter breiten Stellwand zwischen den Schreibtischen kaum mehr Platz benötigt wird. Wir baten die BAgIS, diese Möglichkeit noch einmal zu prüfen, zumal uns bekannt ist, dass eine entspre-

chende Lösung jedenfalls in der BAgIS Ost II in der Eingangszone, einem Großraumbüro auf engstem Raum, bereits verwirklicht worden ist. Unseres Wissens folgten daraufhin keine entsprechenden Maßnahmen der BAgIS.

Ein Betroffener teilte mit, dass in der BAgIS Süd während seines Beratungsgesprächs die Türen zu den Nebenbüros offen gestanden hätten. In den Nebenbüros seien zum gleichen Zeitpunkt weitere Hilfeempfängerinnen und Hilfeempfänger von Mitarbeiterinnen und Mitarbeitern beraten worden, die die Angaben zu Personalien und wirtschaftlicher Situation des Betroffenen mitgehört hätten. Es sei ihm sehr unangenehm gewesen, in Anwesenheit der anderen Personen diese sehr sensiblen Sozialdaten offenzulegen. Wir wiesen die BAgIS einmal mehr darauf hin, dass der Anspruch der Hilfeempfängerinnen und Hilfeempfänger auf Wahrung des Sozialgeheimnisses die BAgIS verpflichte sicherzustellen, dass bei der Beratung nur die jeweils für die Bearbeitung zuständige Person beziehungsweise die zuständigen Personen Kenntnis von den erhobenen Sozialdaten erhalten. Eine Kenntnisnahme von den Daten durch andere Hilfeempfängerinnen und Hilfeempfänger, aber auch durch andere Mitarbeiterinnen und Mitarbeiter der Behörde, ist danach unzulässig. Die BAgIS teilte mit, dass sie ohne die Angabe, um welchen Betroffenen und um welche Mitarbeiterinnen oder Mitarbeiter es sich handele, dazu keine Stellung nehmen könne. Der Hilfeempfänger wollte seinen Namen gegenüber der BAgIS nicht nennen, da er Nachteile befürchtete, sodass diese Angelegenheit nicht weiter aufgeklärt werden konnte.

Im April 2009 wandte sich ein Hilfeempfänger an uns und teilte mit, dass der in der BAgIS Ost II eingesetzte Mitarbeiter eines privaten Sicherheitsdienstes am Empfangstresen seine Sozialdaten mit eingesehen habe. Der Kunde habe dagegen protestiert, woraufhin der Sicherheitsbeauftragte hinter eine Glastür gegangen sei und von dort aus weiter auf den Monitor gesehen habe. Auf unsere Intervention hin wurde dazu von der BAgIS mitgeteilt, dass alle Mitarbeiterinnen und Mitarbeiter und der Sicherheitsbeauftragte darüber belehrt würden, dass dieser die Sozialdaten der Hilfeempfängerinnen und Hilfeempfänger nicht einsehen dürfe. Ein anderer Hilfeempfänger teilte mit, dass der Sicherheitsbeauftragte die Gespräche in den Sachbearbeiterbüros vom Flur aus mit anhören könne, da deren Türen überwiegend offen stünden. Er habe auch Büros betreten und für die Sachbearbeiter Hilfsfunktionen, wie beispielsweise die Anfertigung von Kopien, wahrgenommen. Der Betroffene habe sich darüber bei der BAgIS beschwert, woraufhin ihm mitgeteilt worden sei, dass es sich bei dem Sicherheitsbeauftragten um einen Mitarbeiter der BAgIS handele, der deshalb natürlich auch entsprechend eingesetzt werden dürfe. Die BAgIS hat dies zurückgewiesen, nahm den Vorfall jedoch erneut zum Anlass, ihre Mitarbeiterinnen und Mitarbeiter zu belehren.

**E-Mail-Versand von Sozialdaten**

Als problematisch bewerten wir die Tatsache, dass es der BAgIS trotz entsprechender Versicherungen offenbar nicht gelingt zu verhindern, dass immer wieder hoch sensible Sozialdaten von Hilfeempfängerinnen und Hilfeempfängern ungeschützt per E-Mail versandt werden. Eine Versendung von Sozialdaten in unverschlüsselter Form per E-Mail birgt die Gefahr, dass diese auf ihrem Weg durch das Internet einem unbegrenzten Kreis von unbefugten Dritten bekannt werden. Es ist sogar vorgekommen, dass eine unserer Anfragen in Bezug auf eine datenschutzrechtliche Petition von einem stellvertretenden Geschäftsstellenleiter unverschlüsselt per E-Mail beantwortet worden ist

**Versendung von Akten**

Im Dezember 2008 wandte sich ein Betroffener an uns, der bei der BAgIS Ost II Akteneinsicht beantragt hatte. Die Akten, die von der Widerspruchsstelle der BAgIS ohne Postzustellungsurkunde verschickt worden waren, waren bei ihm nicht angekommen und nicht mehr auffindbar. Die BAgIS teilte mit, dass Akten von dort immer per einfachen Brief verschickt werden. Auf unseren Hinweis, dass dieses Verfahren den Anforderungen des Sozialgesetzbuchs (SGB) an eine dem hohen Schutzbedürfnis von Sozialdaten angemessene Weitergabekontrolle nicht genügt, sicherte die BAgIS zu, Leistungsakten zukünftig nur noch per Einschreiben mit Rückschein, Postzustellungsauftrag oder auf ähnliche Weise zu versenden.

**Rechtswidrige Datenübermittlung an Dritte**

Im Oktober 2008 meldete sich ein Hilfeempfänger und berichtete, von der BAgIS West die Aufforderung erhalten zu haben, sich bei der Bremer Familienkasse der

Arbeitsagentur als Bürohilfskraft zu bewerben. Er habe sich dort per E-Mail beworben und auch eine chronische Krankheit erwähnt. Die Arbeitsagentur habe dann seine Bewerbung an die BAgIS West weitergeleitet mit der Bitte, in Zukunft von derlei Bewerbern verschont zu bleiben. Die BAgIS habe ihn dann angeschrieben mit der Aufforderung, sich zu seinem aktuellen Gesundheitszustand zu äußern. Auf Nachfrage teilte die BAgIS mit, keine Gesundheitsdaten über den Betroffenen gespeichert und die Angelegenheit mit ihm geklärt zu haben. Der Betroffene nahm uns gegenüber von einer weiteren Aufklärung Abstand.

Im April des Berichtsjahres berichtete ein Hilfeempfänger, dass die BAgIS Nord von ihm verlangte, einen Fragebogen von seinem Vermieter ausfüllen zu lassen, der einen Briefkopf der BAgIS, das Aktenzeichen des Hilfeempfängers und Fragen im Zusammenhang mit dem vermieteten Objekt enthielt. Der Hilfeempfänger sah sich in der Lage, die erforderlichen Informationen selbst beizubringen und durch Unterlagen zu belegen. Er wollte den Fragebogen nicht von seinem Vermieter ausfüllen lassen, da er Nachteile befürchtete, wenn sein Vermieter von seiner Hilfebedürftigkeit erführe. Wir konnten bei der BAgIS erreichen, dass der Fragebogen dergestalt umformuliert wurde, dass auf den Briefkopf der BAgIS, die Nennung des Aktenzeichens und die Anschrift von Vermieterinnen und Vermieter verzichtet wird, und er nur in den Fällen eingesetzt wird, in denen sich die erforderlichen Informationen nicht von der Hilfeempfängerin oder dem Hilfeempfänger selbst durch die Vorlage von Unterlagen belegen lassen. Im September beschwerte sich dann ein anderer Hilfeempfänger ebenfalls darüber, dass die BAgIS Nord den ursprünglichen Fragebogen weiter verwendete. Wir wandten uns daraufhin erneut an die BAgIS und fragten, warum die BAgIS nicht ihren Zusagen entsprechend handele und warum der ursprüngliche Fragebogen in der Geschäftsstelle weiterhin verfügbar gehalten werde. Die BAgIS Nord teilte dazu nur mit, dass angewiesen worden sei, nur noch den überarbeiteten Fragebogen zu verwenden und sagte zu, dies im Hause erneut zu thematisieren.

Im September des Berichtsjahres wurde vonseiten der BAgIS mitgeteilt, dass diese plane, sich in Klageverfahren vor Gericht von einer Kanzlei anwaltlich vertreten zu lassen. Die Vertretung sollte alle Prozesshandlungen, wie die Anfertigung von Stellungnahmen, den Abschluss von Vergleichen, die Übersendung von Leistungsakten an das Gericht und so weiter umfassen. Dies sei wegen der erheblichen Klagerückstände erforderlich. Zu diesem Zweck sollte einer Anwaltskanzlei bei der BAgIS ein Raum mit Hardwareausstattung und einem Zugriff auf das Fachverfahren A2LL zur Verfügung gestellt werden. Wir teilten mit, dass wir es für erforderlich halten, die Kanzlei auf die Verpflichtung zur Einhaltung der Vorschriften des Sozialdatenschutzes nach § 78 Absatz 1 SGB X hinzuweisen und durch technische und organisatorische Maßnahmen sicherzustellen, dass der beauftragten Kanzlei nur die zur Aufgabenerfüllung erforderlichen Sozialdaten übermittelt werden. Für die Entscheidung, ob und in welcher Ausgestaltung die Einrichtung von Zugriffsmöglichkeiten auf das Fachverfahren A2LL zulässig ist, ist eine Beschreibung der Bereiche Zugriffsverwaltung, Steuerung und Kontrolle hinsichtlich der Freischaltung für Externe erforderlich, um deren Übersendung wir die BAgIS baten. Später entschied die BAgIS, von der Einrichtung eines elektronischen Zugriffs auf das Fachverfahren A2LL für die Kanzlei abzusehen.

Im Mai schilderte uns ein Hilfeempfänger der BAgIS Ost II, dass er seine Mutter pflege, weshalb die BAgIS von ihm bisher nicht verlangt habe, eine Erwerbsarbeit aufzunehmen. Sein Sohn, mit dem er zerstritten sei und eine gerichtliche Auseinandersetzung um Unterhaltsleistungen führe, habe sich an die BAgIS gewandt und diese aufgefordert, dafür zu sorgen, dass sein Vater sich um die Aufnahme einer Erwerbstätigkeit bemühe. Obwohl bei der BAgIS Ost II bekannt gewesen sei, dass die beiden zerstritten sind, habe die BAgIS dem Sohn mitgeteilt, dass dessen Vater seine Mutter pflege und wann er einen Termin in der BAgIS habe. Sein Sohn hatte dies schriftlich seinem Anwalt mitgeteilt. Vonseiten der BAgIS wurde eingeräumt, dass die Sachbearbeiterin des Betroffenen diese Angelegenheit mit dessen Sohn besprochen habe. Die Mitarbeiterin sei sich der Unzulässigkeit der Übermittlung der Sozialdaten nicht bewusst gewesen, sei daraufhin aber entsprechend belehrt worden. Der Hilfeempfänger hat wegen dieses Vorfalls Strafantrag gegen die Sachbearbeiterin der BAgIS gestellt. Er hat seine Sachbearbeiterin um eine Kopie des Briefes seines Sohnes gebeten, der sich in seiner Akte befindet. Dies lehnte sie ab, woraufhin der Kunde einen Antrag auf Akteneinsicht stellte, zu dem ihm dann mitgeteilt wurde, dass er diese nicht persönlich, sondern nur vertreten durch einen Anwalt erhalten könne. Wir wiesen die BAgIS auf das Recht auf Auskunft des Betrof-

fenen nach § 83 SGB X hin, das durch einen Verweis auf einen vermeintlichen Anwaltszwang in unzulässiger Weise eingeschränkt wird. Die beantragte Akteneinsicht wurde schließlich von der BAgIS gewährt. Im Juli erhielt der Hilfeempfänger ein Schreiben von der BAgIS Süd zum Übergang von Unterhaltsansprüchen seines Sohnes auf die BAgIS. Er rief den zuständigen Sachbearbeiter an, um Fragen zum Inhalt dieses Schreibens zu stellen. Da er sofort nach Nennung seines Namens ohne weitere Prüfung seiner Identität Auskunft erhielt, bat er den Gesprächspartner unter Hinweis auf den Streit mit seinem Sohn, zukünftig keinem Anrufer mehr ohne eindeutige Identitätsfeststellung Informationen aus seiner BAgIS-Akte zu geben. Daraufhin sei ihm mitgeteilt worden, dass sein Sohn wegen des laufenden Unterhaltsverfahrens das Recht habe, Informationen von der BAgIS über ihn zu bekommen. Dies wurde von der BAgIS bestritten; es wurde jedoch zugesichert, zukünftig bei telefonischen Anfragen die Identität des Anrufers zu prüfen.

**Rechtswidrige Datenerhebung**

Im März des Berichtsjahres meldete sich ein Hilfeempfänger und teilte mit, dass ihm durch Akteneinsicht bei der BAgIS Ost II bekannt geworden sei, dass in seiner Akte Bildaufnahmen von seiner Person gespeichert seien. Auf Nachfrage teilte die BAgIS mit, dass ein Mitarbeiter diesen Kunden bei der Ausübung einer bei der BAgIS zu diesem Zeitpunkt nicht bekannten Beschäftigung beobachtet habe. Da er keine Zeugen gehabt habe, habe der Mitarbeiter mit Zustimmung des Betroffenen zur Dokumentation des Vorgangs und zur Sicherung von Beweisen sechs Bildaufnahmen gemacht, die zur Akte genommen worden seien. Da der Kunde nun offenbar mit der Speicherung nicht mehr einverstanden war, er die Beschäftigung eingeräumt habe und sie durch eine Verdienstbescheinigung aktenkundig sei, sei die Speicherung der Bildaufnahmen nicht mehr erforderlich, sodass diese gelöscht wurden. Wir teilten der BAgIS mit, dass hier keine wirksame Einwilligungserklärung des Betroffenen vorgelegen habe, weil der Betroffene weder über den Zweck der Speicherung noch über die Freiwilligkeit seiner Einwilligung oder die Folgen der Verweigerung der Einwilligung aufgeklärt worden war. Ebenso wurde das Schriftformerfordernis nicht eingehalten. Die BAgIS bestätigte daraufhin, in vergleichbaren Fällen zukünftig keine Bildaufnahmen ohne wirksame Einwilligung der Betroffenen mehr zu speichern.

**Rechtswidrige Datenübermittlung an andere öffentliche Stellen**

Im September 2008 meldete sich ein Kunde der ARGE Job-Center Bremerhaven, dem seine ehemalige Partnerin, mit der er ein gemeinsames Kind hat, in ihrem Haus eine Wohnung vermietet hat. Nachdem die ARGE seinen Umzug genehmigt hatte, hatten Mitarbeiter der ARGE unangemeldet mit der Polizei vor seiner Tür gestanden, um mit einem Hausbesuch Sachverhaltsklärung in Bezug auf das Vorliegen einer eheähnlichen Gemeinschaft mit seiner Vermieterin zu betreiben. Der Betroffene verweigerte den Hausbesuch unter Beteiligung der Polizei. Uns gegenüber wurde die Mitnahme eines Polizeibeamten von der ARGE mit einer „zeugenschaftlichen Funktion“ begründet, da der Betroffene mehrfach Dienstaufsichtsbeschwerden gegen Mitarbeiter der ARGE erhoben habe. Unsere Prüfung ergab, dass die Durchführung eines unangemeldeten Hausbesuchs in diesem Fall zwar zulässig war, die Beteiligung der Polizei und die der zugrunde liegenden Übermittlung von Sozialdaten an die Polizei jedoch unzulässig war. Auf unsere Intervention hin sicherte die ARGE schließlich zu, zukünftig auf die Hinzuziehung von Polizeibeamten bei der Durchführung von Hausbesuchen zu verzichten. Ferner berichtete derselbe Betroffene, dass seiner ehemaligen Partnerin vom Amt für Jugend, Familie und Frauen mitgeteilt worden war, dass von dort beabsichtigt sei, ihr die Leistungen nach dem Unterhaltsvorschussgesetz (UVG) zu streichen, da die ARGE telefonisch mitgeteilt habe, dass sie die häusliche Gemeinschaft mit dem Vater ihres Kindes wieder aufgenommen habe. Eine Dokumentation dieses Telefonats befand sich nicht in der Leistungsakte der ARGE. Diese sah sich daher nicht in der Lage festzustellen, ob von dort eine Datenübermittlung an das Jugendamt erfolgt ist. Auf unsere Aufforderung hin bestätigte die ARGE, ihre Mitarbeiterinnen und Mitarbeiter anzuweisen, entsprechende Datenübermittlungen zukünftig in den Akten zu dokumentieren, um im Nachhinein eine Beauskunftung und Überprüfung der Rechtmäßigkeit der Datenübermittlung zu ermöglichen.

### 7.4 Datenschutzfragen im Zusammenhang mit dem Sozialticket

Im Januar 2009 informierte uns die Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales über die Planungen zur Durchführung einer Marktanalyse für die

Einführung eines Sozialtickets in der Stadtgemeinde Bremen. Im Rahmen dieser Marktanalyse sollte von einem Marktforschungsunternehmen eine telefonische Befragung durchgeführt werden, um unter der Zielgruppe, den Empfängerinnen und Empfängern von Grundsicherung und Arbeitslosengeld II, den Bedarf und die daraus entstehenden Kosten zu ermitteln. Dafür sollten vom Amt für Soziale Dienste (AfSD) und der BAgIS für eine Stichprobe von 7.000 Personen aus der Zielgruppe Daten zu Name, Adresse, Telefonnummer, Art des Leistungsbezugs, Geschlecht und Haushaltsgröße an die Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales übermittelt werden. Diese sollte die Betroffenen dann schriftlich über die geplante Telefonbefragung durch das Marktforschungsunternehmen informieren und dazu auffordern, der Datenübermittlung an das Marktforschungsunternehmen zu widersprechen, wenn sie damit nicht einverstanden seien. Die Namen und Telefonnummern der Leistungsempfängerinnen und -empfänger, die keinen Widerspruch einlegten, sollten dem Marktforschungsunternehmen zur Durchführung der telefonischen Befragungen übermittelt werden. Wir teilten der Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales mit, dass die Übermittlung der Sozialdaten der Hilfeempfängerinnen und -empfänger vom Amt für Soziale Dienste und der BAgIS an die senatorische Behörde ohne Einwilligung der Betroffenen nicht zulässig ist. Die weitere Datenübermittlung von der senatorischen Behörde an das Marktforschungsunternehmen ist ebenfalls nicht zulässig, weil nach § 75 Sozialgesetzbuch (SGB) X Sozialdaten zum Zweck der Planung im Sozialleistungsbereich nur an eine öffentliche Stelle übermittelt werden dürfen. Für diese Übermittlung bedarf es dann ebenfalls einer Einwilligung der Betroffenen; die Einräumung einer Widerspruchsmöglichkeit reicht insoweit nicht aus. Daraufhin nahm die senatorische Behörde von diesem Verfahren Abstand und plante stattdessen, die Befragung durch das Marktforschungsunternehmen an einem Stand in den Räumen des Amtes für Soziale Dienste und der BAgIS direkt auf freiwilliger Basis unter den Wartenden durchzuführen. Wir begrüßten diese Entscheidung.

Im August wandte sich dann die BAgIS an uns und bat um datenschutzrechtliche Prüfung eines Berechtigungsausweises, der für die Beantragung des Sozialtickets ausgestellt werden sollte. Dieser Berechtigungsausweis sollte ein Foto, Name, Geburtsdatum und Adresse der oder des Berechtigten sowie einen Stempel der Ausgabestelle, also der BAgIS oder dem Amt für Soziale Dienste, enthalten. Er sollte bei Fahrkartenkontrollen den Kontrolleurinnen und Kontrolleuren der Bremer Straßenbahn Gesellschaft (BSAG) vorgelegt werden. Wir teilten der BAgIS unsere datenschutzrechtlichen Bedenken gegen dieses Verfahren mit, die darin begründet waren, dass es sich bei einer Fahrkartenkontrolle nicht verhindern ließe, dass der Kontrolleurin oder dem Kontrolleur und den umstehenden Fahrgästen bekannt würde, dass es sich bei der oder dem Berechtigten um eine Hilfeempfängerin oder Hilfeempfänger handelt. Das hielten wir für unzumutbar, zumal es sich bei den Umstehenden häufig um Bekannte, Nachbarinnen oder Nachbarn, Kolleginnen oder Kollegen oder um Mitschülerinnen oder Mitschüler handeln wird. Die Betroffenen hätten dann Schwierigkeiten, ihren Leistungsbezug in ihrem Umfeld geheim zu halten. Daher forderten wir, dass für den Fahrausweis des Sozialtickets eine neutral gestaltete Kundenkarte verwendet wird, sodass verhindert werden kann, dass Umstehende auf diesem Weg von dem Hilfebezug der oder des Betroffenen erfahren. Gegen die Verwendung des Lichtbildes und des Namens der Betroffenen, die sich auch auf anderen Zeitkarten, wie dem Jobticket oder dem Semesterticket befinden, erhoben wir keine Bedenken. Wir stellten jedoch die Erforderlichkeit der Verwendung des Geburtsdatums und der Adresse infrage. Nach umfassenden weiteren Beratungen wurde schließlich entschieden, dass den Berechtigten von der BAgIS und dem Amt für Soziale Dienste eine Bestätigung über den Leistungsbezug ausgestellt wird, eine sogenannte Grüne Karte. Die Grüne Karte kann bei den Verkaufsstellen der BSAG für die Ausstellung der Kundenkarte für das Sozialticket vorgelegt werden. Die Kundenkarte selbst soll in ihrem Design ähnlich wie andere Kundenkarten der BSAG gestaltet und nur durch unauffällige Markierungen als Sozialticket gekennzeichnet werden. Zudem wurde für das Ticket ein anderer Name gewählt, um eine Stigmatisierung der Betroffenen zu verhindern.

### 7.5 Kooperationsprojekte des Amtes für Soziale Dienste

Wie in den vergangenen Jahren war auch im Jahr 2009 unsere Zusammenarbeit mit dem Amt für Soziale Dienste (AfSD), Abteilung Junge Menschen und Familie, stark geprägt vom Einfluss des Falls Kevin im Oktober 2006. Obwohl im Fall Kevin Informationsdefizite der beteiligten Stellen nicht vorlagen, sondern bei ausreichen-

der Informationslage wohl Defizite im Handeln mit ursächlich für den Tod des kleinen Jungen gewesen sind, wurde als Konsequenz aus diesem Fall die Vernetzung der Beteiligten aus dem Bereich der Jugendhilfe mit dem näheren Umfeld von Kindern kontinuierlich vorangetrieben. Es liegt auf der Hand, dass der gewünschten engen Zusammenarbeit aller Beteiligten, wie Jugendhilfe, Schule, Polizei, freie Träger, Kindertagesstätten, Kinderärzte, Gesundheitsamt und so weiter datenschutzrechtliche Grenzen gesetzt sind.

Im Dezember 2008 bat uns ein Sozialzentrum des Amtes für Soziale Dienste um Beratung hinsichtlich einer Kooperationsvereinbarung mit Kinder- und Jugendärztinnen und -ärzten im Stadtteil. In dem vorgelegten Entwurf dieser Vereinbarung war unter anderem geregelt, dass in den Fällen, in denen von Kinderärztinnen und Kinderärzten bei der Behandlung ein Hilfebedarf festgestellt wird, sich diese an die Kindertagesstätte oder die Schule, den Kinder- und Jugendgesundheitsdienst und die Stadtteilleitung des Sozialzentrums wenden sollten. In Fällen von drohender Kindeswohlgefährdung sollten die Kinderärztinnen und -ärzte den Kinder- und Jugendnotdienst einschalten. Über Maßnahmen der Jugendhilfe sollten die Kinderärztinnen und -ärzte eine Rückmeldung erhalten. Wir teilten dem Sozialzentrum mit, dass dieser Entwurf der Vereinbarung in wesentlichen Teilen nicht mit den Vorschriften zum Sozialdatenschutz und der ärztlichen Schweigepflicht vereinbar ist. Grundsätzlich ist eine Datenübermittlung durch die Kinderärztin oder den Kinderarzt nur zulässig, wenn die Betroffenen nach umfassender Aufklärung über Zweck und Umfang der Datenübermittlung eine wirksame Schweigepflichtentbindungserklärung erteilt haben. Wird diese Erklärung verweigert, darf nur bei Vorliegen der sehr engen Voraussetzungen des rechtfertigenden Notstands nach § 34 Strafgesetzbuch (StGB) ausnahmsweise eine Datenübermittlung auch gegen den Willen – jedoch grundsätzlich nicht ohne Wissen – der Betroffenen erfolgen. Anderenfalls liegt ein Verstoß gegen die ärztliche Schweigepflicht vor, der nach § 203 StGB strafbewehrt ist. Die Rückmeldung über Maßnahmen des Jugendamtes an die behandelnden Ärztinnen und Ärzte ohne Einwilligung der Betroffenen stellt eine Verletzung des Sozialgeheimnisses nach § 35 SGB I dar. Die Vereinbarung wurde schließlich soweit überarbeitet, dass die behandelnden Ärztinnen und Ärzte lediglich bei Herausnahme des Kindes aus der Familie darüber informiert werden, dass das Kind nicht mehr im Stadtteil wohnt und daher nicht mehr in die Behandlung kommen werde. Für alle Datenübermittlungen zwischen den Ärztinnen oder Ärzten und dem Sozialzentrum sollten Einwilligungs- beziehungsweise Schweigepflichtentbindungserklärungen der Betroffenen eingeholt werden. Nur soweit diese nicht erteilt werden und die Voraussetzungen des § 34 StGB vorliegen, sollten Datenübermittlungen gegen den Willen der Betroffenen erfolgen. Die Vereinbarung wurde im März 2009 in Kraft gesetzt.

Im Februar 2009 wandte sich dieses Sozialzentrum erneut an uns mit der Bitte, eine ähnliche Kooperationsvereinbarung mit Schulen im Stadtteil zu begleiten. Diese Vereinbarung sieht bei bekannt werden von schulischen Problemen beim Jugendamt beziehungsweise erzieherischen oder familiären Problemen in der Schule einen Datenaustausch und eine Abstimmung von weiteren Maßnahmen zwischen Schule und Jugendamt vor. Der Datenaustausch wurde auch hier, soweit gesetzlich nicht erlaubt, auf eine Einwilligungserklärung der Schülerinnen und Schüler beziehungsweise Eltern gestützt. In Fällen von akuter Kindeswohlgefährdung soll eine Datenübermittlung an das Jugendamt auch gegen den Willen – grundsätzlich aber nicht ohne Wissen – der Betroffenen erfolgen. Die Vereinbarung war bis Redaktionsschluss noch nicht abschließend abgestimmt.

Zurzeit befindet sich außerdem die Vereinbarung zur Sicherstellung des Schutzauftrages bei Kindeswohlgefährdung gemäß § 8 a SGB VIII in der Abstimmung, bei der es ebenfalls um einen Datenaustausch zwischen dem Jugendamt und den Schulen in Bremen bei Anzeichen auf Kindeswohlgefährdung geht.

Die Verhandlungen zum Projekt „Ablaufplan Kinderschutz“, mit dem eine Vereinbarung zum Datenaustausch zwischen Kinderärztinnen und -ärzten und dem Jugendamt getroffen werden sollte, sind zurzeit ausgesetzt worden. Eine Einigung konnte wegen der Weigerung der beteiligten Ärzte zur Beachtung der datenschutzrechtlichen Vorschriften bis jetzt nicht erzielt werden.

### 7.6 Runder Tisch Heimerziehung

Im September wandte sich das Amt für Soziale Dienste (AfSD) an uns und bat um Beratung im Hinblick auf datenschutzrechtliche Fragestellungen bei der Aufarbei-

tung des Heimunrechts in den Fünfziger- und Sechzigerjahren. Im Zusammenhang mit dem „Runden Tisch Heimerziehung“ auf Bundesebene war in Bremen ein Telefon für Opfer des Heimunrechts eingerichtet worden. Betroffene melden sich dort mit unterschiedlichen Anliegen, wie beispielsweise der Bitte um Akteneinsicht oder konkreten Fragen zu ihrer Vergangenheit. Diese Anliegen und Fragen werden im Amt für Soziale Dienste zurzeit anhand eines standardisierten Fragebogens gesammelt. Die Betroffenen werden am Telefon nach ihrem Einverständnis über die Benachrichtigung des Trägers ihres ehemaligen Kinderheims über ihre Anfrage gefragt. Eine Kontaktaufnahme zu den privaten Trägern ist grundsätzlich erforderlich, da im AfSD keine Heimakten, sondern nur die Akten über die Fürsorgeerziehung oder die freiwillige Erziehungshilfe vorhanden sind. Die Heimakten sind teilweise noch seit dem Jahr 1943 bei den Trägern vorhanden. Ein Heimträger hatte eine Kooperation mit einem Wissenschaftler aufgenommen, der bereits begonnen hatte, die Akten zu sichten und Gespräche mit Betroffenen zu führen. Wir teilten mit, dass vor der Gewährung von Akteneinsicht in Bezug auf Daten Dritter einzelfallbezogen zu prüfen ist, ob diese zu schwärzen sind, weil deren schutzwürdige Interessen an der Geheimhaltung überwiegen. Dies wäre wohl nicht der Fall bei Mitarbeiterinnen und Mitarbeitern des Heimes, könnte aber im Einzelfall bei anderen Betroffenen, wie Eltern, andere Kinder, Geschwister, zutreffen. Bei der Anfertigung von Kopien der Akte für die Betroffenen sollten diese Daten grundsätzlich geschwärzt werden. Eine Datenübermittlung zu Forschungszwecken durch das Amt für Soziale Dienste ist nur bei Vorliegen einer wirksamen Einwilligungserklärung zulässig, da bei entsprechend sensiblen Daten über körperliche beziehungsweise sexuelle Misshandlung und so weiter einer Übermittlung ansonsten schutzwürdige Belange der Betroffenen entgegenstehen. Die Einwilligung muss schriftlich eingeholt werden. Vorzugswürdig wäre aber eine Anonymisierung der Akten vor der Weitergabe an die Forscherinnen und Forscher, weil dann auf eine Kontaktaufnahme mit den Betroffenen verzichtet werden kann. Auch die Akten der privaten Träger dürfen ohne Einwilligung nicht ungeschwärzt an Wissenschaftlerinnen und Wissenschaftler weitergegeben werden. Vonseiten des Amtes für Soziale Dienste und des privaten Trägers wurde zugesagt, diese Anforderungen einzuhalten und an die anderen betroffenen Heimträger weiterzugeben. Dafür sollte ein Datenschutzkonzept erarbeitet werden, in dem die oben genannten Anforderungen für alle Beteiligten beschrieben sind, und ein Formular für eine Einwilligungserklärung zur Weitergabe der Akten zu Forschungszwecken erstellt werden. Beides sollte mit uns abgestimmt werden. Bis Redaktionsschluss haben wir keine Unterlagen erhalten.

### 7.7 Gesundheit Nord gGmbH / Kommunale Kliniken in Bremen

Im Januar 2009 unterrichtete uns der behördliche Datenschutzbeauftragte der Gesundheit Nord gGmbH (GeNo) und des Klinikums Bremen-Mitte über das Vorhaben, für alle vier kommunalen Kliniken in Bremen eine zentrale Datenverarbeitung bei der Gesundheit Nord gGmbH einzuführen. Später erfuhren wir, dass die gesamte Informationstechnik, alle patientenfernen Dienste, das Personal, mit Ausnahme der Ärztinnen und Ärzte sowie der Pflegerinnen und Pfleger, alle Geräte, die gesamte Krankenhausverwaltung, Patientenabrechnungen und so weiter der Kliniken in die Holding Gesundheit Nord gGmbH ausgelagert werden sollen. Wir wiesen darauf hin, dass ein solches Vorhaben eine Reihe von Fragen in Bezug auf die Zulässigkeit der damit verbundenen Datenverarbeitungen und die technische Umsetzung der Anforderungen des Krankenhausdatenschutzgesetzes aufwirft, die vor Beginn der Übertragungen geklärt werden müssten. § 7 Absatz 2 Bremisches Datenschutzgesetz (BremDSG) schreibt vor, dass die verantwortlichen Stellen vor der Einführung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden sollen, eine Risikoanalyse durchführen und ein Datenschutzkonzept erstellen müssen sowie die Kontrolle der behördlichen Datenschutzbeauftragten zu gewährleisten haben. Die Einhaltung dieser Anforderungen sowie die Beteiligung der Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) wurden uns zugesagt. Wir erhielten jedoch in den folgenden Monaten trotz regelmäßiger Nachfragen nach schriftlichen bewertbaren Unterlagen keine weiteren inhaltlichen Informationen, die uns eine Bewertung beziehungsweise datenschutzrechtliche Begleitung des Vorhabens ermöglichten. Stattdessen wurden uns immer wieder Unterlagen mit allgemeinen Ausführungen übersandt, die in diesem Sinne nicht bewertungsfähig waren. Vonseiten der GeNo wurde wiederholt versichert, dass selbstverständlich eine rechtzeitige Information erfolgen werde. Ende Juni teilte dann die Geschäftsführung der GeNo mit, dass die Konzeption zur Auslagerung der Informationstechnik in die GeNo bereits abgeschlossen und alle Daten-

schutzfragen gelöst seien. Der Aufsichtsrat werde die Umsetzung dieses Konzeptes beschließen, mit der sukzessive ab Juli 2009 begonnen werden solle. Für den Bereich der Auslagerung der Patientenabrechungen werde erst in den kommenden drei Monaten ein Grobkonzept erarbeitet. Auf unseren Einwand, dass eine Beteiligung der LfDI entgegen der Zusagen nicht erfolgt sei, sicherte der Geschäftsführer der GeNo zu, uns das Konzept zur Auslagerung der Informationstechnik, die datenschutzrechtliche Risikoanalyse, die Unterlagen zur Vorabkontrolle sowie das Datenschutzkonzept kurzfristig zu übersenden. In Bezug auf die geplante Auslagerung der Patientenabrechnungen wiesen wir auf die erhebliche datenschutzrechtliche Relevanz bei der Weitergabe der der ärztlichen Schweigepflicht unterliegenden Patientendaten hin und baten auch diesbezüglich um rechtzeitige Unterrichtung. Eine Übersendung der zugesagten Unterlagen erfolgte nicht; später wurde eingeräumt, dass diese noch gar nicht erstellt worden waren. Es wurde jedoch versichert, dass daran gearbeitet werde. Im September erhielten wir vom Geschäftsführer der GeNo die Auskunft, dass sich die Auslagerung der Informationstechnik zeitlich verzögere und dass vor deren Umsetzung ein Datenschutzkonzept übersandt und die Datenschutzfragen mit der LfDI abgestimmt würden. Kurz darauf stellte sich heraus, dass die Personalabteilung bereits zum Oktober 2009 und die Finanzabteilung, die auch die Patientenabrechnungen betreibe, zum November 2009 in die GeNo übertragen worden sind. Bis zum Jahresende sollten alle Betriebsübergänge abgeschlossen sein. Im Oktober wurde uns dann ein Konzept übersandt, das zwar technische Beschreibungen, jedoch keine Erläuterungen zu den geplanten Datenflüssen enthielt, sodass wir auch dieses Konzept als nicht bewertungsfähig zurückweisen mussten.

### 7.8 Weitergabe eines sozialmedizinischen Gutachtens durch den Medizinischen Dienst der Krankenkassen

Im Januar meldete sich ein Bürger, der beim Medizinischen Dienst der Krankenkassen (MDK) zwecks Erstellung eines sozialmedizinischen Gutachtens zur Frage der Arbeitsunfähigkeit untersucht worden war. Das Gutachten des MDK, das Ausführungen enthielt, deren Richtigkeit vom Betroffenen zum Teil bezweifelt wurden, war an seinen behandelnden Orthopäden und teilweise – ohne Vorgeschichte und Befund – an seine Krankenkasse versandt worden. Vonseiten des MDK wurde mitgeteilt, dass für die Versendung des Gutachtens an den Orthopäden das Einverständnis des Betroffenen eingeholt worden sei, was vom Betroffenen bestritten wurde. Zudem berichtete der Betroffene, dass sein Arbeitgeber bestätigt habe, telefonisch vom MDK über den Inhalt des Gutachtens informiert worden zu sein, was vonseiten des MDK bestritten wurde. Leider ließ sich der Sachverhalt von uns nicht vollständig aufklären. Die Weitergabe des Gutachtens ist aus datenschutzrechtlicher Sicht wie folgt zu beurteilen: § 277 Absatz 1 Sozialgesetzbuch (SGB) V erlaubt lediglich die Weitergabe des Ergebnisses der Begutachtung und der erforderlichen Angaben über den Befund an die Krankenkasse. Den Leistungserbringern, über deren Leistungen der MDK eine gutachtliche Stellungnahme abgegeben hat, darf der MDK das Ergebnis der Begutachtung und, wenn der Betroffene nicht widerspricht, auch die erforderlichen Angaben über den Befund mitteilen. Die Weitergabe des vollständigen Gutachtens erlaubt § 277 Absatz 1 SGB V nicht. An den Arbeitgeber des Versicherten darf der MDK keine Sozialdaten übermitteln. Deshalb ist festzustellen, dass es für die Übermittlung des Gutachtens – ohne Vorgeschichte und Befund – an die Krankenkasse des Betroffenen keine Rechtsgrundlage gab, weshalb diese unzulässig war. Auch die Einholung einer Einwilligung des Versicherten zur Übermittlung des vom MDK erstellten sozialmedizinischen Gutachtens an die Krankenkasse wäre nicht zulässig, weil der Krankenkasse auf diesem Weg weitere Möglichkeiten der Datengewinnung eröffnet würden, die über die nach dem Willen des Gesetzgebers vorgesehenen hinausgehen. Das SGB V regelt für die Krankenkassen abschließend, in welchen Fällen Sozialdaten erhoben werden dürfen (§§ 284 ff SGB V). Eine darüber hinausgehende Einwilligungslösung sieht das SGB V nicht vor. In Bezug auf die Übermittlung des vollständigen Gutachtens an den Orthopäden war es nicht ausreichend, dass die Weitergabe „im Einvernehmen“ mit dem Betroffenen erfolgte. Im Gegensatz zur Übermittlung an die Krankenkasse könnte eine Datenübermittlung vom MDK an den behandelnden Arzt zwar grundsätzlich auf eine Einwilligungserklärung des Betroffenen gestützt werden. Soweit diese vom MDK eingeholt wird, muss sie aber den Anforderungen des § 67 b Absatz 2 SGB X entsprechen. Danach ist er auf den Zweck der Datenübermittlung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung muss freiwillig sein und bedarf grundsätzlich der Schriftform. Da hier eine solche schriftliche

Erklärung vom Betroffenen nicht eingeholt wurde, war auch die Datenübermittlung an den behandelnden Orthopäden unzulässig. Auch bei solchen Übermittlungen sollte aus den oben genannten Gründen davon abgesehen werden, ohne Initiative des behandelnden Arztes eine Einwilligung zur Übermittlung des Gutachtens vom Betroffenen einzuholen. Im vorliegenden Fall, in dem laut Gutachten das Begutachtungsergebnis dem Betroffenen nicht mitgeteilt worden ist, gilt dies umso mehr, da er hier noch nicht einmal wusste, welche Sozialdaten über ihn weitergegeben werden sollten. Die Berücksichtigung der oben genannten Grundsätze wurde vom MDK für die Zukunft zugesagt. Der Betroffene hat Strafanzeige gegen die verantwortliche Ärztin beim MDK erstattet.

### 7.9 Einsatz von externen Beraterinnen und Beratern zur Qualitätsprüfung durch die AOK Bremen / Bremerhaven

Bereits im Jahr 2006 bekamen wir von einem Sanitätshaus den Hinweis, dass von Krankenkassen externe Beraterinnen und Berater – Hilfsmittelberater – eingesetzt werden, denen Sozialdaten der Versicherten übermittelt werden, damit sie bei den betroffenen, meist älteren Versicherten unangekündigte Hausbesuche durchführen, um die Erforderlichkeit und Angemessenheit der verordneten Hilfsmittel zu überprüfen. Auf Nachfragen wurde uns vonseiten der Allgemeinen Ortskrankenkasse (AOK) Bremen / Bremerhaven mitgeteilt, dass von ihr eine Firma beauftragt worden sei, in Einzelfällen die Zweckmäßigkeit und Wirtschaftlichkeit von verordneten Hilfsmitteln zu prüfen. Der Firma würden zu diesem Zweck alle für die Prüfung erforderlichen Sozialdaten der betroffenen Versicherten übermittelt. Zur Datenerhebung bei den Versicherten sei diese Firma vertraglich nicht verpflichtet, gegebenenfalls würden jedoch die Lieferanten befragt. Als Rechtsgrundlage für die Übermittlung der Sozialdaten an die Hilfsmittelberater benannte die AOK die §§ 12 und 197 a Sozialgesetzbuch (SGB) V. Wir teilten der AOK unsere Rechtsauffassung dazu mit: § 12 Absatz 1 Satz 1 SGB V gibt den Krankenkassen vor, dass Leistungen ausreichend, zweckmäßig und wirtschaftlich sein müssen. Eine Datenübermittlungs- oder eine Datenerhebungsbefugnis enthält § 12 SGB V jedoch nicht. Auch die Vorschrift des § 197 a SGB V enthält keine Befugnis für eine Datenübermittlung beziehungsweise -erhebung. Diese Vorschrift sieht die Schaffung einer organisatorischen Einheit bei der Krankenkasse vor, die Fällen und Sachverhalten im Zusammenhang mit der Nutzung der Finanzmittel nachgeht. Die Einheit nimmt Kontrollbefugnisse nach § 67 c Absatz 3 SGB X wahr. § 67 c Absatz 3 SGB X enthält lediglich die Fiktion, dass eine Speicherung, Veränderung oder Nutzung von Sozialdaten für bestimmte Verwaltungsmaßnahmen, unter anderem für Kontrollen durch die verantwortliche Stelle, keine Zweckänderung darstellt. Das bedeutet, dass die in der AOK vorhandenen Sozialdaten für die dort genannten Zwecke, hier also die Kontrolle durch die Einheit nach § 197 a SGB V, genutzt werden können. Datenerhebungen regelt § 67 c SGB X nicht. Ebenso werden keine externen Kontrollbefugnisse geschaffen. Vielmehr haben die organisatorischen Einheiten nach § 197 a Absatz 1 Satz 1 SGB V internen Charakter, sodass lediglich innerhalb der Organisation vorhandene personenbezogene Daten für Kontrollzwecke genutzt werden dürfen. Diese Daten müssen auf anderer Grundlage, wie zum Beispiel § 284 Absatz 1 Satz 1 Nummer 8 SGB V unter Berücksichtigung von §§ 275 ff SGB V, gewonnen worden sein. Die Übermittlung von Sozialdaten an Externe wäre nur bei Vorliegen einer wirksamen Einwilligungserklärung der Betroffenen nach § 67 b Absatz 2 SGB X zulässig, soweit dadurch nicht die Zuständigkeit des Medizinischen Dienstes der Krankenkassen (MDK) umgangen wird. Da die Beurteilung medizinischer Fragen Aufgabe des MDK ist, darf eine Datenübermittlung an Externe auf Einwilligungsbasis nur zum Zweck der Beurteilung rein technischer Fragen erfolgen. Zulässig wäre nach § 127 Absatz 3 SGB V lediglich die Übermittlung der erforderlichen Sozialdaten in pseudonymisierter Form an andere Leistungserbringer zum Zweck der Einholung von Preisangeboten; ein Personenbezug darf durch den Empfänger dabei jedoch nicht herstellbar sein. Wir baten die AOK zu bestätigen, zukünftig auf eine Übermittlung und Erhebung von Sozialdaten ohne wirksame Einwilligung der Betroffenen zum Zweck der Prüfung von Notwendigkeit und Wirtschaftlichkeit von Hilfsmittelverordnungen zu verzichten. Die AOK weigerte sich, eine entsprechende Bestätigung abzugeben und legte ein Gutachten einer Rechtsanwaltskanzlei vor, das zum Ergebnis kam, dass die Beauftragung privater Firmen zum Zweck der Überprüfung der Zweckmäßigkeit und Wirtschaftlichkeit von Hilfsmitteln zulässig ist. Wir wandten uns daraufhin an die Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales und baten diese, in ihrer Funktion als Aufsichtsbehörde für die AOK auf die Einhaltung der Vorschriften zum Sozialdaten-

schutz hinzuwirken. Die Senatorin schloss sich unserer Rechtsauffassung an und konnte die Abgabe der geforderten Bestätigung von der AOK erreichen.

### 7.10 Auslagerung der Abrechnungsprüfung durch die Kassenärztliche Vereinigung Bremen

Im Oktober 2007 wandte sich eine Laborgemeinschaft an uns und teilte mit, dass die Kassenärztliche Vereinigung Bremen (KVHB) deren Abrechnungen und Befunde zum Zweck der Durchführung der Plausibilitätsprüfung und der Prüfung der sachlichen und rechnerischen Richtigkeit nach § 106 a Sozialgesetzbuch (SGB) V an die Kassenärztliche Vereinigung Bayern (KVB) übermittelt. Auf Nachfrage teilte die KVHB mit, dass sie die KVB, die ein Kompetenzzentrum für Laborüberprüfungen betreibt, mit der Überprüfung der Abrechnungen beauftragt habe. Wir wiesen die KVHB darauf hin, dass wir für die Weitergabe der im Rahmen der Abrechnungsprüfung erhobenen Sozialdaten an die KVB keine Rechtsgrundlage sehen. Eine Datenverarbeitung im Auftrag nach § 80 SGB X kommt nicht in Betracht, da die vollständige Überprüfung der sachlichen und rechnerischen Richtigkeit an die KVB übertragen werden soll, sodass es nicht um die Übertragung von Hilfsfunktionen handelt, sondern um die Übertragung einer Aufgabenerfüllung (Funktionsübertragung), die von § 80 SGB X nicht erfasst ist. Die Voraussetzungen von § 88 SGB X für eine wirksame Aufgabenübertragung sind hier ebenfalls nicht erfüllt, weil diese Regelung auf die KVHB, die kein Leistungsträger im Sinne von § 12 SGB I ist, nicht anwendbar ist. Die KVHB teilte mit, dass unsere Auffassung dort nicht geteilt werde. Da die gesetzliche Aufgabe und die datenschutzrechtliche Verantwortung bei der KVHB verbleiben und der KVB keine eigenen Entscheidungsbefugnisse eingeräumt würden, würde entgegen unserer Auffassung nur eine Hilfsfunktion übertragen, sodass die Voraussetzungen einer Auftragsdatenverarbeitung nach § 80 SGB X vorlägen. Diese Auftragsdatenverarbeitung sei auch entsprechend § 80 Absatz 3 SGB X der Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales als Aufsichtsbehörde angezeigt worden, die keine Bedenken erhoben habe. Wir wandten uns daraufhin an den Bayerischen Landesbeauftragten für den Datenschutz mit Sitz in München (LfD Bayern), der bei der KVB vor Ort die Datenverarbeitung im Kompetenzzentrum prüfte. Dabei stellte er fest, dass das „K(B)V Kompetenzzentrum Labor“ bei der KVB die Kassenärztlichen Vereinigungen der Länder auf deren Anfrage und in deren Auftrag bei der Abrechnungsprüfung nach §§ 106 f SGB V unterstützen soll. Der Service des Kompetenzzentrums umfasst die allgemeine und spezielle Beratung bis hin zur Erstellung von Vorschlägen für einzelne oder sämtliche Laborabrechnungs- beziehungsweise Prüfbescheide einer Kassenärztlichen Vereinigung. Dafür sollte zwischen allen Kassenärztlichen Vereinigungen der Länder und der Kassenärztlichen Bundesvereinigung (KBV) die Gründung einer Arbeitsgemeinschaft (ARGE) nach § 77 Absatz 6 SGB V in Verbindung mit § 94 Absatz 1 a SGB X vereinbart werden, die mit der Aufgabenerfüllung betraut werden und dafür ihrerseits einen Auftrag an die KVB erteilen sollte. Der LfD Bayern kam zu dem Ergebnis, dass die Plausibilitätsprüfung von Laborleistungen nicht in rechtlich zulässiger Weise über eine ARGE auf die KVB übertragen werden kann. Die ARGE kann zwar zur gegenseitigen Unterrichtung, Abstimmung, Koordinierung und Förderung der engen Zusammenarbeit der beteiligten Stellen dienen, die Übertragung von Aufgaben der an der ARGE beteiligten Einrichtungen ist nach den Vorschriften des Sozialgesetzbuchs jedoch nicht zulässig. Ebenfalls unzulässig wäre eine Einzelbeauftragung der KVB durch eine kassenärztliche Vereinbarung, da weder die Voraussetzungen von § 80 SGB X (Auftragsdatenverarbeitung) noch nach § 88 SGB X (Funktionsübertragung) erfüllt sind. Diese Rechtsauffassung wird von uns geteilt. Wir haben die KVHB daher aufgefordert zu bestätigen, dass sie die Übermittlung von Abrechnungs- und Befunddaten an die KVB unverzüglich einstellt. Die KVHB teilte daraufhin mit, dass sie zwar vorläufig keine weiteren Abrechnungs- und Befunddaten an die KVB übermitteln werde. In der Sache teile sie die dargelegte Rechtsauffassung jedoch nicht und sei der Auffassung, dass der LfD Bayern seine Kompetenz überschritten habe. Daher würde sie abwarten, bis das Bundesministerium für Gesundheit sich in dieser Sache äußern werde.

### 7.11 Weitergabe von Sozialdaten an Hilfsmittelhersteller durch die AOK Bremen / Bremerhaven

Im Dezember 2008 meldete sich eine Versicherte der Allgemeinen Ortskrankenkasse (AOK) Bremen / Bremerhaven bei uns. Die AOK hatte ihre Sozialdaten – Name, Adresse, Geschlecht, Krankenversicherungsnummer, Telefonnummer, Bezug von

Inkontinenzmitteln – an eine Firma weitergegeben, die Inkontinenzmittel vertreibt. Diese Firma hatte die Sozialdaten ihrerseits an ein Callcenter weitergegeben, das von ihr mit der Kundenberatung beauftragt worden sei. Insbesondere dieser Umstand beunruhigte die Betroffene, die befürchtete, dass ihre Sozialdaten unbefugten Dritten zur Kenntnis gelangen könnten. Die AOK teilte mit, mit dem Hilfsmittelhersteller einen Vertrag über die Versorgung mit Inkontinenzmitteln nach § 127 Sozialgesetzbuch (SGB) V abgeschlossen zu haben. Sie veranlasste auf unsere Anfrage hin unverzüglich die Löschung der Daten der Versicherten bei dem vom Lieferanten beauftragten Callcenter und teilte mit, die betroffenen Versicherten und deren bisherige Leistungserbringer schriftlich darüber informiert zu haben, dass sie zukünftig nur noch die Kosten für Inkontinenzmittel erstatten werde, die von ihrer Vertragspartnerin bezogen werden. Sie habe den Versicherten angekündigt, deren Sozialdaten an den vertraglich verpflichteten Leistungserbringer zu übermitteln, wenn sie nicht innerhalb von zwei Wochen widersprächen. Wir wiesen die AOK darauf hin, dass es für die Übermittlung von Sozialdaten an Dritte einer Rechtsgrundlage bedarf. Rechtsgrundlage für die Übermittlung von versichertenbezogenen Sozialdaten durch Krankenkassen ist § 284 Absatz 3 Satz 1 SGB V. Danach dürfen die rechtmäßig erhobenen und gespeicherten versichertenbezogenen Daten nur für die Zwecke der Aufgaben nach Absatz 1 in dem jeweils erforderlichen Umfang verarbeitet und genutzt werden, für andere Zwecke, soweit dies durch Rechtsvorschriften des Sozialgesetzbuchs angeordnet oder erlaubt ist. Diese Voraussetzungen lagen hier nicht vor. Die Übermittlung der Daten war insbesondere auch nicht zum Zweck der Erbringung von Leistungen an Versicherte erforderlich. § 33 Absatz 6 Satz 2 SGB V bestimmt insoweit, dass für den Fall, dass die Krankenkasse Verträge nach § 127 Absatz 1 über die Versorgung mit bestimmten Hilfsmitteln geschlossen hat, die Versorgung durch einen Vertragspartner erfolgt, der den Versicherten von der Krankenkasse zu benennen ist. Auch nach § 127 Absatz 5 Satz 1 SGB V haben die Krankenkassen ihre Versicherten über die zur Versorgung berechtigten Vertragspartner und auf Nachfrage über die wesentlichen Inhalte der Verträge zu informieren. Eine gesetzliche Erlaubnis für die Weitergabe von Sozialdaten an Hilfsmittelversorger gibt es nicht. Zwar wäre die Datenübermittlung bei Vorliegen einer wirksamen Einwilligungserklärung zulässig gewesen; die Eröffnung einer Widerspruchsmöglichkeit gegen die Datenübermittlung genügt diesen Anforderungen jedoch nicht. Erforderlich wäre die Abgabe einer ausdrücklichen Erklärung. Wir baten die AOK Bremen / Bremerhaven, zukünftig in gleichgelagerten Fällen ohne wirksame Einwilligung der Betroffenen keine versichertenbezogenen Sozialdaten mehr an Hilfsmittelversorger zu übermitteln. Die AOK bezweifelte zunächst die von uns vertretene Rechtsauffassung, dass die Eröffnung einer Widerspruchsmöglichkeit nicht den Anforderungen an eine wirksame Einwilligungserklärung nach § 67 b Absatz 2 SGB X genügt und teilte mit, dass sie die Übermittlung der Sozialdaten für erforderlich halte, um einen nahtlosen Übergang bei der Versorgung mit Inkontinenzmitteln sicherzustellen, sicherte aber schließlich zu, entsprechende Datenübermittlungen zukünftig nur noch bei Vorliegen einer rechtmäßigen Einwilligungserklärung der Betroffenen vorzunehmen.

In diesem Zusammenhang ist zu berichten, dass uns ein Pflegeheimträger mitteilte, dass sich der von der AOK beauftragte Lieferant für Inkontinenzmittel an Pflegeheime gewandt hatte und dort um die Übermittlung von konkreten gesundheitsbezogenen Informationen zum Bedarf und Verbrauch von Inkontinenzmitteln der betroffenen Bewohnerinnen und Bewohner in personenbezogener Form gebeten hatte. Der Träger nahm unsere Anregung auf, darauf hinzuwirken, dass die Pflegeheime die Informationen nur in anonymisierter Form an den Hilfsmittellieferanten weitergeben.

### 7.12 Datenverarbeitung im Zusammenhang mit der Impfung gegen H1N1 (Schweinegrippe)

Ende August des Berichtsjahres meldete sich die Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales bei uns und bat um Prüfung der geplanten Datenverarbeitung im Zusammenhang mit der Impfung der Bremer Bevölkerung gegen das H1N1-Virus (Schweinegrippe). Die Impfung sollte vom Gesundheitsamt teilweise selbst, teilweise vertreten durch niedergelassene Ärztinnen und Ärzte, Betriebsärztinnen und -ärzte und den Medizinischen Dienst der Krankenkassen (MDK) als Verwaltungshelfer durchgeführt werden. Vor der Impfung sollte von allen Impfwilligen ein ärztlicher Dokumentationsbogen ausgefüllt werden, auf dem Name, Adresse, Geburtsdatum, Daten zur Angehörigkeit einer für die Impfung prioritären

Gruppe, wie zum Beispiel Beschäftigung in einer Gesundheits- oder Pflegeeinrichtung, der Berufsfeuerwehr oder der Polizei, oder Vorliegen einer schweren Krankheit abgefragt werden. Auch für die Impfung relevante Gesundheitsinformationen, wie zum Beispiel zu Allergien, Schwangerschaft, Medikamenteneinnahme, gehörten dazu. Auf diesem Dokumentationsbogen sollte zudem zum Zweck der Abrechnung vom impfenden Arzt oder von der impfenden Ärztin Name und Praxisstempel, das Impfdatum und die Chargen-Nummer vermerkt werden. Weiter enthielt der Bogen die Erläuterung, dass die persönlichen Daten ausschließlich zur Durchführung, Dokumentation und Abrechnung der Impfung verwendet würden. Diese Dokumentationsbögen sollten nach der Impfung im Gesundheitsamt direkt an die Geschäftsstelle Impfung bei der Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales, Abteilung Gesundheitswesen, weitergeleitet werden. Dort sollte die Zahl der Impfungen zu Abrechnungszwecken ermittelt und die Bögen anschließend für zehn Jahre aufbewahrt werden. Bei Impfungen durch niedergelassene Ärztinnen und Ärzte sollten die Bögen zuerst an die Kassenärztliche Vereinigung weitergegeben werden, damit diese die Impfungen anonym mit dem Fonds der Krankenkassen abrechnen könne und anschließend zur senatorischen Dienststelle weitergeleitet werden. Wir erhoben gegen die zehnjährige Aufbewahrung der Dokumentationsbögen bei der senatorischen Dienststelle zum Zweck der ärztlichen Dokumentation letztendlich keine Bedenken, da eine entsprechend lange Dokumentation ärztlicher Unterlagen nach der Berufsordnung für Ärzte vorgesehen ist und diese nicht bei den impfenden Ärztinnen und Ärzte geführt werden sollte, da diese lediglich als Verwaltungshelfer des öffentlichen Gesundheitsdienstes tätig werden. Dafür wurde die Datenschutzerklärung auf dem Dokumentationsbogen insoweit geändert, dass erläutert wird, dass die Daten bei der Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales, Abteilung Gesundheit, für zehn Jahre aufbewahrt werden. Da jedoch die Abrechnung mit dem Fonds der Krankenkassen anonym erfolgen sollte, dafür von der Kassenärztlichen Vereinigung also keine personenbezogenen Daten der Patienten benötigt wurden, wirkten wir darauf hin, dass auf eine Übersendung der Dokumentationsbögen an die Kassenärztliche Vereinigung verzichtet wird. Stattdessen wird der Kassenärztlichen Vereinigung von der senatorischen Behörde nur noch die Anzahl der erfolgten Impfungen pro Ärztin beziehungsweise Arzt mitgeteilt.

### 7.13 Bevölkerungsumfrage Gesundheit

Im April des Berichtsjahres informierte uns die Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales über Planungen zur Durchführung der zweiten Bevölkerungsumfrage Gesundheit im Rahmen der Gesundheitsberichterstattung. Dafür wurde im Mai ein Fragebogen mit ungefähr 30 Fragen zur gesundheitlichen und sozialen Situation an 5.000 repräsentativ ausgewählte Bürgerinnen und Bürger in Bremen und Bremerhaven versandt. Die Teilnahme war freiwillig, die Befragung war im Anschreiben als anonym angekündigt. Für den Versand der Fragebögen und der Erinnerungsschreiben wurden bei den Meldeämtern Vor- und Familiennamen, akademischer Grad, Geschlecht, Adresse, Geburtsjahr und Staatsangehörigkeit erhoben. Diese Daten wurden für den Druck der Fragebögen an die Hausdruckerei der Senatorin für Finanzen übermittelt. Wir rügten, dass die Versendung in elektronischer Form unverschlüsselt erfolgte und wiesen darauf hin, dass die Weitergabe der Adressdaten an die Hausdruckerei der Senatorin für Finanzen unzulässig war, da es keine Rechtsgrundlage gibt, die diese Datenübermittlung erlaubt und auch keine Auftragsdatenverarbeitung vereinbart worden war. Bei der Durchsicht der Unterlagen stellten wir fest, dass auf den Fragebögen eine Identifikationsnummer aufgedruckt war, die bei der senatorischen Behörde zusammen mit den personenbezogenen Daten gespeichert wurde. Dadurch wäre leicht eine Zusammenführung der Fragebögen mit den Identitätsdaten der Teilnehmerinnen und Teilnehmer möglich, sodass die Befragung entgegen der Darstellung im Anschreiben an die Teilnehmerinnen und Teilnehmer nicht anonym war. Später erreichten uns diesbezüglich auch mehrere Beschwerden von Bürgerinnen und Bürgern, die sich getäuscht fühlten und wegen der hoch sensiblen Fragen sehr aufgebracht waren. Die senatorische Behörde teilte mit, dass die auf den Fragebögen aufgedruckten Identifikationsnummern lediglich verwendet würden, um festzustellen, welche Teilnehmerin und welcher Teilnehmer geantwortet hätten, um den Versand der Erinnerungsschreiben zu steuern. Wir regten an, wenn auf die Identifikationsnummer nicht verzichtet werden solle, diese wenigstens zukünftig nicht mehr auf den Fragebogen, sondern auf den Rückumschlag aufzudrucken, um eine sofortige Trennung von Identifikationsnummer und Inhaltsdaten zu ermöglichen und

damit die Möglichkeit der Zusammenführung zu verringern. Dies wollte die senatorische Behörde für die zukünftige Befragung nicht bestätigen. Zudem rügten wir, dass über dieses Verfahren gegenüber den Betroffenen keine Transparenz hergestellt, sondern vielmehr der Anschein einer anonymen Befragung erzeugt wurde. Vonseiten der senatorischen Behörde wurde schließlich zugesagt, die potenziellen Teilnehmerinnen und Teilnehmer bei der nächsten Befragung im Anschreiben darüber zu informieren, dass es sich lediglich um eine pseudonymisierte Befragung handelt und zu welchem Zweck hier eine Identifikationsnummer verwendet wird. Zudem wurde versichert, die Unterlagen vor der nächsten Befragung mit uns abzustimmen.

## 8. Bildung und Wissenschaft, Kultur

### 8.1 Medien- und Datenschutzkompetenz

Ein besonderer Schwerpunkt unserer Arbeit in den nächsten Jahren wird es sein, die Medien- und Datenschutzkompetenz der Bürgerinnen und Bürger zu stärken. Gerade die neuen Medien, insbesondere das Internet, bieten den Menschen neue Erfahrungs- und Lernbereiche. Es entwickelt sich eine neue gesellschaftliche Kultur der Kommunikation. Diese birgt jedoch auch erhebliche Risiken durch die Verbreitung privater und intimer Daten in sozialen Netzwerken, wie SchülerVZ, StudiVZ, facebook und anderen. Das Gleiche gilt für die sonstige Nutzung des Internets, zum Beispiel Einkauf und Recherche, weil jede Aktivität im Internet Spuren hinterlässt, ohne dass die Betroffenen in der Lage sind, die weltweite und vielfältige Weiterverwendung und -verknüpfung ihrer Daten mit anderen Datenverarbeitungssystemen im Internet zu verhindern. Insoweit ist es unsere Aufgabe, an der Entwicklung von Medienkompetenz im Hinblick auf den Datenschutz mitzuwirken. Nach einer Analyse der derzeitigen Aktivitäten zu diesem Thema in Bremen haben wir festgestellt, dass sich bereits eine Vielzahl von Akteuren diesem Thema widmet, zum Beispiel das Landesinstitut für Schule, die Landesmedienanstalt und das ServiceBureauJugendinformation. Nach ersten Gesprächen mit diesen Einrichtungen haben wir vereinbart, uns gegenseitig zu unterstützen durch die nicht nur zielgruppenorientierte Erstellung und Herausgabe von Flyern und Plakaten sowie die Ergänzung von Lehrplänen und die Mitwirkung an Veranstaltungen zu diesem Thema.

Mit dem Thema Medienkompetenz befasst sich auch die Arbeitsgruppe „Schule / Bildung“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter dem Vorsitz des rheinland-pfälzischen Landesbeauftragten für den Datenschutz. Beschränkten wir uns in der Arbeitsgruppe zunächst auf die Medien- und Datenschutzkompetenz von Schülerinnen und Schülern, wird es nunmehr immer bedeutsamer, auch die übrigen Bürgerinnen und Bürger anzusprechen, weil inzwischen diverse Personengruppen in sozialen Netzwerken kommunizieren, sodass die damit verbundenen Risiken auch für sie in gleicher Weise bestehen. Aus diesen Gründen sieht es die Arbeitgruppe als notwendig an, die Medien- und Datenschutzkompetenz beziehungsweise den Datenschutz als Bildungsaufgabe für alle Menschen zu verstehen.

### 8.2 Aufforderung an Kindertagesstätten zur Übermittlung einer Liste über Kinder für die CITO-Sprachstandserhebung

Ein freier Träger von Kindertagesstätten unterrichtete uns darüber, dass die Senatorin für Bildung und Wissenschaft von allen Kindertageseinrichtungen per E-Mail eine Liste über Kinder angefordert hatte, die in diesem Jahr an der CITO-Sprachstandserhebung teilnehmen sollten. Auf dem vorgefertigten E-Mail-Formular hätten die Einrichtungen die vollständigen Namen, Geburtsdaten, Geschlecht und Adressen der Kinder einzutragen.

Auf unsere Anfrage erklärte das Ressort, der nach dem Bremischen Schulgesetz vorgesehene Sprachstandstest vor der Einschulung solle in den Kindertagesstätten durchgeführt werden, weil sich die überwiegende Anzahl der Kinder in diesen Einrichtungen befänden. Eine vorherige namensmäßige Erfassung erleichtere die notwendige Zuordnung der Testpersonen in der Kontrolldatei der Schulverwaltung. Da eine Rechtsgrundlage zur Übermittlung dieser Daten durch die Kindertagesstätten gesetzlich nicht geregelt ist, seien die Träger gebeten worden, die Zustimmung der Eltern beziehungsweise der Erziehungsberechtigten einzuholen. Der Auf-

forderung an die Träger der Kindertagesstätten sei auch der Brief an die Eltern beigefügt worden. Dieser enthielt aber lediglich den Hinweis, dass die Daten einen „reibungslosen und datengeschützten Ablauf garantieren“ sollten, und die am Ende des Elternbriefs aufgeführte Einwilligungserklärung.

Auf unsere weitere Nachfrage erklärte die Senatorin für Bildung und Wissenschaft, Träger von Kindertagesstätten hätten den Wunsch gehabt, die Kinder durch Erzieherinnen und Erzieher zum Test in die Schule bringen zu lassen, weil die Testergebnisse zuverlässiger seien, wenn die Kinder von vertrauten Personen begleitet würden. Zur Gewährleistung eines reibungslosen Ablaufes für die Kindertagesstätten sollten Gruppentermine vergeben werden, zu denen die Erzieherinnen und Erzieher immer mit einer Gruppe von Kindern zum Test in die Schule gehen könnten. Hierfür seien die Listen erforderlich gewesen. Diese Erklärung haben wir aus datenschutzrechtlicher Sicht für ausreichend erachtet.

Zur unverschlüsselten E-Mail-Übersendung der Listen erklärte das Ressort, dies sei als aufwandsarme Alternative zur Übergabe der Listen anlässlich einer Besprechung mit den Trägern von Kindertageseinrichtungen angeregt worden. Inzwischen sei klargestellt, dass derartige Daten nicht mehr unverschlüsselt übermittelt werden dürfen.

Mit dem Ressort haben wir vereinbart, anlässlich der nächsten anstehenden Sprachstandserhebung eine datenschutzrechtliche Verbesserung des Verfahrens zu erreichen, insbesondere hinsichtlich der Anforderungen an eine wirksame Einwilligung der Eltern in die Datenübermittlung durch die Kindertagesstätten.

### 8.3 Umgang mit personenbezogenen Daten der Bewerberinnen und Bewerber im Berufungsverfahren der Universität Bremen

Im Berichtsjahr wurde uns bekannt, dass die Universität Bremen im Rahmen ihrer Berufungsverfahren zur Neu- oder Wiederbesetzung vakanter Stellen für Hochschullehrerinnen und -lehrer sogenannte „Assessment-Center-Verfahren“, also psychologische Eignungs- und Auswahltests, zur Beurteilung der außerfachlichen Eignung der in die engere Wahl gekommenen Bewerberinnen und Bewerber einsetzt. Mit der Durchführung dieser Assessment-Center-Verfahren wurde ein externes Unternehmen beauftragt. Mitarbeiterinnen und Mitarbeiter des Unternehmens begutachten in einem mehrstündigen, aus unterschiedlichen Übungsteilen bestehenden Verfahren das jeweilige Verhalten der ausgewählten Bewerberinnen und Bewerber und versuchen, hieraus generelle Rückschlüsse auf einzelne Persönlichkeitsmerkmale, etwa die emotionale Stabilität, Selbstbewusstsein, Kontaktfähigkeit, Gewissenhaftigkeit, Belastbarkeit und so weiter, zu ziehen. Darüber hinaus werden eine Selbsteinschätzung der Persönlichkeit und persönliche Schwächen der Bewerberinnen und Bewerber abgefragt. Die Ergebnisse dieses Assessment-Center-Verfahrens werden in einem ausführlichen Bericht zusammengestellt und liefern ein weitgehendes – auch psychologisches – Persönlichkeitsbild der Bewerberinnen und Bewerber.

Dieser Bericht wird in ungekürzter, detaillierter Fassung an alle Mitglieder der Berufungsgremien, insgesamt bis zu 29 Personen – ohne Vertreter –, darunter auch an zwei wissenschaftliche Fachkräfte und an zwei Studierende in der Berufungskommission, weitergeleitet.

Wir haben die Universitätsleitung darauf aufmerksam gemacht, dass die Weitergabe dieses sensible personenbezogene Daten enthaltenden Berichts in ungekürzter Fassung an einen dermaßen großen Personenkreis geltendes Datenschutzrecht in massiver Weise verletzt. Unter anderem wiesen wir darauf hin, dass in der Einwilligung der Bewerberinnen und Bewerber in die Teilnahme am Assessment-Center-Verfahren, auf die sich die Universität Bremen in erster Linie beruft, bereits nicht ohne weiteres eine Einwilligung in die Übermittlung sämtlicher im Verfahren erhobener Daten an alle Mitglieder der Berufungsgremien liegt. Im Übrigen wäre eine Einwilligung in die Datenübermittlung aufgrund der Besonderheiten der vorliegenden Bewerbungssituation nach geltendem Datenschutzrecht eindeutig unwirksam. Gemäß § 3 Absatz 3 Bremisches Datenschutzgesetz (BremDSG) ist eine Einwilligung nämlich nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Da die Bewerberinnen und Bewerber seitens der Universität aus dem weiteren Bewerbungsverfahren herausgenommen würden, wenn sie mit der Durchführung eines Assessment-Center-Verfahrens nicht einverstanden wären, ihre Einwilligung also alternativlos ist, könnte von einer tatsächlichen Freiwilligkeit, wie

sie im Datenschutzrecht vorausgesetzt wird, nicht die Rede sein. Zudem ist die Befugnis zur Erhebung personenbezogener Daten im Bewerbungsverfahren nach anwendbarem bremischen Beamtenrecht gesetzlich beschränkt. Diese bewusste gesetzliche Erhebungsschranke kann auch nicht durch die Einholung einer Einwilligung umgangen werden. Im Übrigen sind die erhobenen personenbezogenen Daten der Bewerberinnen und Bewerber wie Personalaktendaten zu behandeln, für die nach ständiger höchstrichterlicher Rechtsprechung und entsprechender gesetzlicher Umsetzung besondere Vertraulichkeitsschutzprinzipien gelten, so etwa die strikte und enge Begrenzung der zu diesen Daten zugangsbefugten Personen. Diese gesetzlichen Schutzprinzipien können nicht etwa durch eine universitäre Berufungsordnung, die ihrer Rechtsnatur nach lediglich einfaches Satzungsrecht darstellt und daher dem höherrangigen Gesetzesrecht, namentlich dem Beamtenrecht, untergeordnet ist, ausgehebelt werden. Nicht zuletzt wird auch die spezielle Erhebungsvorschrift des § 20 Absatz 4 BremDSG verletzt.

Bislang zeigte sich die Universität nicht einsichtig, hält vielmehr an ihrer rechtswidrigen Praxis fest.

### 8.4 Speicherung von Daten durch die Theater Bremen GmbH

Durch eine Eingabe wurden wir darauf hingewiesen, dass die Theater Bremen GmbH beim Verkauf von Theaterkarten für einzelne Aufführungen an der Theaterkasse Daten ihrer Kunden erhebt. Soweit die Kundinnen und Kunden damit einverstanden sind, werden von ihnen Namen, Adressen und Telefonnummern selbst in den Fällen erhoben, in denen die Karten an den Kassen bar bezahlt werden. Die Theater Bremen GmbH begründete die Erhebung der Daten zunächst mit der Absicht, die Theaterbesucherinnen und Theaterbesucher bei einer Vorstellungsänderung, Vorstellungsabsage oder Ähnlichem rechtzeitig informieren zu wollen.

Erst eine nochmalige Nachfrage bei der Theater Bremen GmbH zu diesem Thema ergab, dass die Speicherung der Kundendaten nicht etwa auf die jeweilige Aufführung begrenzt ist, sondern erheblich darüber hinausgeht. Wie uns mitgeteilt wurde, beträgt die Speicherdauer tatsächlich zehn Jahre. Die Daten würden nicht nur für die jeweilige Aufführung gespeichert, sondern auch, um die Kundinnen und Kunden über weiter vergleichbare Programmpunkte, zum Beispiel die nächste Verdi-Oper, zu informieren. Die Theater Bremen GmbH verfüge über einen überregionalen Kundenstamm, bei dem zwischen den einzelnen Theaterbesuchen Jahre liegen könnten. Die betreffenden Kundinnen und Kunden seien auf Informationen der Theater Bremen GmbH angewiesen, da sie zum Beispiel keine Bremer Zeitungen lesen könnten.

Zu diesen Erläuterungen wiesen wir darauf hin, dass die Theater Bremen GmbH personenbezogene Daten nur im Rahmen der Vorschriften des Bremischen Datenschutzgesetzes (BremDSG) verarbeiten darf. Gemäß § 22 Absatz 3 BremDSG sind personenbezogene Daten zu löschen, wenn zum einen die Speicherung unzulässig ist oder zum anderen die Kenntnis der Daten für die verantwortliche Stelle zur rechtmäßigen Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Eine ausreichende Rechtsgrundlage ergibt sich für die Datenverarbeitung in diesem Fall aus den Bestimmungen des Bremischen Datenschutzgesetzes nicht. Sollen die Kundendaten mit der Einwilligung der Betroffenen verarbeitet werden, so setzt dies neben der Freiwilligkeit der Einwilligung hier insbesondere voraus, dass die Kundinnen und Kunden über die Zwecke der Verarbeitung ihrer Daten informiert sind. Selbst wenn die Betroffenen die Einwilligung in die Speicherung ihrer Daten erteilt haben, ist es sinnvoll, dass es eine angemessene Speicherdauer gibt, nach deren Ablauf die Kundinnen und Kunden ihre Einwilligung für die weitere Speicherung ihrer Daten erteilen müssten.

Eine von der Theater Bremen GmbH vorgeschlagene Speicherdauer von fünf Jahren wurde von uns für zu lang befunden. Eine Dauer von einem Jahr, maximal zwei Jahren sollte ausreichen.

Um hinsichtlich der Speicherung der Besucherdaten zu einem datenschutzkonformen Verfahren zu gelangen, haben wir die Theater Bremen GmbH schließlich um die Entwicklung eines Formulars gebeten, mit dem die Theaterkundinnen und -kunden in die Verarbeitung ihrer Daten einwilligen können. Aus einem gleichzeitig zu erstellenden Informationsschreiben sollten die genannten Zwecke der Datenverarbeitung (Benachrichtigung über Verschiebungen oder Ausfälle von Veranstaltun-

gen und Information über vergleichbare Angebote), die Speicherdauer und ein jederzeitiges Widerspruchsrecht für die Kundinnen und Kunden eindeutig hervorgehen.

Die Theater Bremen GmbH ist unserer Empfehlung nach einer Speicherdauer von zwei Jahren bislang nicht gefolgt. Das für die Einwilligung vorgeschlagene Formular und das zur Gewährleistung der Transparenz der Datenverarbeitung erbetene Informationsschreiben sind bisher nicht vorgelegt worden.

## 9. Umwelt, Bau und Verkehr

### 9.1 Nachweis zur Prüfung einer sozialen Härte für Ausnahmefahrten innerhalb der Umweltzone

Für Anträge auf Ausnahmefahrten in der Umweltzone wegen einer sozialen Härte stellte das Amt für Straßen und Verkehr im Internet Antragsfragebögen zur Verfügung. Dem Antrag sollten die Einkommenssteuererklärung sowie die letzten drei Gehaltsabrechungen, der eine Vielzahl von sozialen Daten enthaltende Bescheid über den Bezug von Grundsicherung oder Arbeitslosengeld II sowie eine Kopie des Personalausweises beigefügt werden. In dem auszustellenden Ausweis, der hinter die Windschutzscheibe gelegt werden muss, sollten Name und Anschrift des Halters aufgeführt werden.

Nach einer daraufhin erfolgten Abstimmung zwischen der Behörde und uns, die von einer öffentlichen Berichterstattung begleitet wurde, wurde das Verfahren datenschutzkonform umgestaltet. Berechtigte, deren Einkommen unterhalb der festgelegten Grenzen liegt, brauchen dies nur noch mit einem Dokument nachzuweisen. Insbesondere müssen Bezieher von Sozialleistungen lediglich ein Dokument vorlegen, das nur den Bezug der Sozialleistung nachweist. Schließlich enthält der Ausweis für die Windschutzscheibe – ähnlich wie bei Anwohnerparkausweisen – nur das Kraftfahrzeugkennzeichen und die Geltungsdauer.

### 9.2 Einführung einer gesplitteten Entwässerungsgebühr

Die Stadtgemeinde Bremen beabsichtigt die Einführung einer gesplitteten Entwässerungsgebühr. Demnach sollen Eigentümer von mit Abwasseranschlüssen versehenen Grundstücken ab einem festzulegenden Versiegelungsgrad mit der neuen Entwässerungsgebühr belastet werden. Dabei lasse sich der Versiegelungsgrad nur mit Luftbilddaten und einer besonderen Software ermitteln. Hierzu haben wir dem Ressort vorgeschlagen, die fehlenden Rechtsgrundlagen zur erforderlichen Datenverarbeitung zu schaffen.

Daraufhin hat der Senator für Umwelt, Bau, Verkehr und Europa den Entwurf zur Änderung ortsentwässerungsrechtlicher Vorschriften vorgelegt, der unter anderem die Befliegung des Stadtgebietes mit anschließender Erstellung der Geodaten für die Berechnung der neuen Gebühr erlaubt. Außerdem soll durch eine Änderung des Ortsgesetzes erlaubt werden, die bei den Entsorgungsbetrieben zur Berechnung der Abfallgebühren gespeicherten Daten einer anderen Behörde zu übermitteln, wenn dies zu deren rechtmäßiger Aufgabenerfüllung erforderlich ist.

Wir haben das Ressort aufgrund der Unbestimmtheit der vorgeschlagenen Formulierung darauf hingewiesen, dass Datenübermittlungsregelungen unter anderem den verfassungsmäßigen Grundsätzen der Normenklarheit und Zweckbindung entsprechen müssen. In dem Ortsgesetz muss präzise festgelegt werden, an welche Behörde die Daten zu welchem Zweck übermittelt werden dürfen. Daher haben wir vorgeschlagen, im Ortsgesetz die Übermittlung für die bei den Entsorgungsbetrieben gespeicherten Daten im erforderlichen Umfang an die für die Erhebung der Niederschlagswassergebühr zuständigen Behörde zuzulassen.

### 9.3 Bremisches Geodatenzugangsgesetz

Nach der europäischen INSPIRE-Richtlinie (Richtlinie zur Geodateninfrakstruktur) haben die Mitgliedstaaten der Europäischen Union eine europäische Geodateninfrastruktur aufzubauen. Ziel ist die Interoperabilität von Geodaten und Geodatendiensten, um den Zugang zu und die Nutzung von Geodaten (Daten mit Bezug zu einem bestimmten oder geografischen Gebiet) für Bürgerinnen und Bürger, Verwaltung und Wirtschaft zu vereinfachen. Dazu legte uns der Senator für Umwelt, Bau, Verkehr und Europa den Entwurf eines Bremischen Geodatenzugangsgesetzes

(BremGeoZG) zur Stellungnahme vor. Der Entwurf setzt die organisatorischen, technischen und rechtlichen Vorgaben der Richtlinie um.

Zunächst wurde von uns gemeinsam mit dem Ressort die Auffassung vertreten, dass durch das Gesetz bereichsspezifische Regelungen über die Verarbeitung personenbezogener Geodaten geschaffen werden sollten. Demgegenüber entschied das Ressort später, dass alle öffentlichen Stellen im Rahmen ihrer Verantwortung selbst über die Übermittlung personenbezogener Geodaten an Dritte und den Zugang zu Informationen durch Bürgerinnen und Bürger entscheiden sollen. Demzufolge hat sich das Ressort mit unserer Unterstützung dazu entschlossen, dass lediglich hinsichtlich der Beschränkung des Zugangs zu personenbezogenen Geodaten die entsprechenden Regelungen des Bremischen Umweltinformationsgesetzes (BremUWG) gelten sollen. Das finden wir unbedenklich, weil bereits der Bund und einige andere Länder gleiche Regelungen haben. Das Gesetz ist am 10. Dezember 2009 in Kraft getreten.

## 10. Finanzen

### 10.1 Vom Finanzamt Bremen-West fehlgeleitete Unterlagen

Im Mai des Berichtsjahres wandte sich ein Ehepaar an uns und teilte mit, dass es mit einem Anschreiben des Finanzamtes seine Steuerbelege zurückbekommen sollte, jedoch die Steuerunterlagen einer fremden Person übersandt bekommen habe. Das Ehepaar schickte die falschen Unterlagen ans Finanzamt zurück, und wir wandten uns zur Sachverhaltsaufklärung an das zuständige Finanzamt Bremen-West. Daraufhin wurde von der Amtsleitung die Verfahrensweise im Finanzamt hinsichtlich der Erstellung der Anschreiben zur Rückgabe der Steuererklärungsbelege genau geschildert. Ebenso wurde erläutert, wie es zu der Verwechslung der Belege kommen konnte. Die Verwechslung von Adresse und Unterlagen ließ sich folgendermaßen aufklären: Das EDV-Programm zur Bearbeitung der Steuerfälle ermöglicht das Erstellen von Standardschreiben, in die automatisch die Adresse und Steuernummer des Steuerpflichtigen aus dem gespeicherten Datenbestand übertragen werden. Ruft während der Bearbeitung eines Steuerfalls am PC beispielsweise eine andere steuerpflichtige Person an, so ist es für die Bearbeiterin oder den Bearbeiter gegebenenfalls erforderlich, den Fall der anrufenden Person am PC aufzurufen, um sich mit ihrem Anliegen auseinandersetzen zu können. Kommt es nach Beendigung des Telefonats noch zu weiteren Störungen oder Unterbrechungen, so kann es passieren, dass der Fall der Anruferin beziehungsweise des Anrufers im EDV-Programm nicht wieder geschlossen wird. Ein Standardschreiben, wie im vorliegenden Fall für die Rücksendung der eingereichten Belege an die Steuerpflichtigen, wird dann automatisch mit den Daten des geöffneten Falles erstellt und nicht mit den Daten derjenigen, deren Erklärung tatsächlich bearbeitet wird. Das Anschreiben wird ausgedruckt, mit den Unterlagen in einen Briefumschlag mit Sichtfenster gesteckt und zur Post aufgegeben. Im vorliegenden Fall handelte es sich ganz offensichtlich um diese Verkettung unglücklicher Umstände. Die Amtsleitung hat den Fall zum Anlass genommen, die Bediensteten auf mögliche Fehlerquellen hinzuweisen und sie aufgefordert, streng auf die Einhaltung datenschutzrechtlicher Belange zu achten.

### 10.2 Schuldnerverzeichnis im Finanzamt Bremen-Mitte

Im Jahr 2009 erfolgte die datenschutzrechtliche Prüfung des Schuldnerverzeichnisses des Finanzamts Bremen-Mitte. Das Schuldnerverzeichnis des Finanzamts umfasst ungefähr 16.000 personenbezogene Datensätze. Um die Vollstreckung im Finanzamt zu effektivieren, wird in diesem Schuldnerverzeichnis eine Abfrage der Vollstreckungsstelle vorgenommen, um festzustellen, ob eine eidesstattliche Versicherung (EV) von Steuerschuldnern abgegeben wurde. Ist die Abfrage positiv, so wird seitens des Finanzamts keine Vollstreckungsmaßnahme unternommen. Per Suchfunktion können die 64 Mitarbeiterinnen und Mitarbeiter der Vollstreckungsstelle alle Schuldnerinnen und Schuldner einsehen. Vor Einsatz dieses Schuldnerverzeichnisses gab es 37 monatliche Listen, die von allen Beschäftigten der Vollstreckungsstelle zur Aufgabenerfüllung eingesehen werden mussten. Die Aktualität der ältesten Monatsliste warf hier datenschutzrechtliche Bedenken auf. In der jetzt realisierten Lösung handelt es sich um eine einzige Liste, die in elektronischer Form ausgegeben wird.

Die Einrichtung eines parallelen Schuldnerverzeichnisses mittels elektronischen Abdrucks von den jeweiligen Amtsgerichten in Bremen wird durch die §§ 915 ff. Zivilprozessordnung (ZPO) in Verbindung mit der Schuldnerverzeichnisverordnung (SchuVVO) unter bestimmten Voraussetzungen zugelassen. Aus datenschutzrechtlicher Sicht haben wir darauf hingewiesen, dass die Vollstreckungsstelle keine Auskünfte an Dritte erteilen darf.

Bei dem Schuldnerverzeichnis innerhalb der Vollstreckungsstelle handelt es sich durch die Nutzung im Rahmen der Abfrage von eidesstattlichen Versicherungen um eine zulässige Datenverarbeitung. Gemäß § 7 Absatz 4 Bremisches Datenschutzgesetz (BremDSG) sind technische und organisatorische Maßnahmen zu treffen, die insgesamt die Datensicherheit der Schuldnerangaben gewährleisten, insbesondere sind die an den Zugriff und die Aktualisierung der Daten des Schuldnerverzeichnisses gestellten Anforderungen gemäß § 10 Absatz 4 Satz 2, Absatz 3 SchuVVO und § 7 Absatz 4 BremDSG zu beachten. Daher sind Maßnahmen zur Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle zu treffen, und es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Ferner sind an den automatisierten Abruf mittels Suchformular für eidesstattliche Versicherungen zur Klärung der Frage, ob eine eidesstattliche Versicherung beim jeweiligen Amtsgericht vorliegt oder nicht, besondere Anforderungen entsprechend § 18 SchuVVO zu stellen. Problematisch war in diesem Zusammenhang die Integrität der Daten – Zugriff auf die Daten, Eingabe und Löschung der Daten – hinsichtlich der Veränderungsmöglichkeit durch die 64 Mitarbeiterinnen und Mitarbeiter der Vollstreckungsstelle. Einer unabsichtlichen oder missbräuchlichen Eintragung oder Löschung einer Schuldnerin oder eines Schuldners beziehungsweise einer anderen Veränderung der Schuldnertabelle wird nach unserem Hinweis durch Schutzmaßnahmen entgegengewirkt. Der behördliche Datenschutzbeauftragte teilte uns mit, dass zwischenzeitlich eine Verfahrensbeschreibung erstellt worden ist und er die Vorabkontrolle nach § 7 Absatz 2 BremDSG vorgenommen hat.

### 10.3 Reorganisation der Berechtigungen im SAP

Seit 2003 wird SAP in der bremischen Kernverwaltung flächendeckend eingesetzt. Seinerzeit haben wir die Einführung von SAP im Rahmen des Projektes Chipsmobil begleitet (vergleiche 26. Jahresbericht, Ziffer 13.3).

Derzeit nutzen ungefähr 1.700 Benutzerinnen und Benutzer das System SAP. Durch Übergang des Rechenzentrumsbetriebs von der ID Bremen GmbH zu Dataport (vergleiche 30. Jahresbericht, Ziffer 6.1) fand eine Standortmigration der Systeme nach Hamburg statt. Die zugrunde liegenden Konzepte waren somit überarbeitungsbedürftig.

Die Senatorin für Finanzen hat daher das Projekt „Rebe – Reorganisation der Berechtigungen im SAP-Mandanten 100“ ins Leben gerufen. Wir beteiligen uns an diesem Projekt in den Arbeitspaketen „Berechtigungskonzept“, „Kritische Berechtigungen“ und „Support“.

Bereits zum Start des Projektes haben wir allerdings deutlich gemacht, dass eine alleinige Überarbeitung der Berechtigungskonzepte nicht die Gesamtsicherheit der SAP-Systeme gewährleisten kann. Darüber hinaus ist aus unserer Sicht die Überarbeitung des IT-Rahmenkonzeptes, des Datenschutzkonzeptes und des IT-Betriebskonzeptes zwingend erforderlich. Zwar wurde uns durch die Senatorin für Finanzen mitgeteilt, dass das Projekt derzeit nur auf die Reorganisation der Berechtigungen ausgerichtet ist, wir empfehlen allerdings dringend, entsprechende Folgeprojekte aufzusetzen. Wir gehen davon aus, dass die Senatorin für Finanzen unserer Empfehlung folgen wird.

### 10.4 Novellierung des Bremischen Beamtengesetzes

Im Rahmen der Föderalismusreform sind die Gesetzgebungskompetenzen zwischen Bund und Ländern grundlegend neu geordnet worden. Für den Bereich des öffentlichen Dienstrechts wurden die Gesetzgebungskompetenzen für die Beamtinnen und Beamten sowie für die Richterinnen und Richter neu geregelt. Aus diesem Grund hat die Senatorin für Finanzen uns den Entwurf eines Gesetzes zur Neuregelung des Beamtenrechts in der Freien Hansestadt Bremen zur Stellungnahme vorgelegt. Datenschutzrechtlich bedeutsam ist hierbei die Novellierung des Bremischen Beamtengesetzes (BremBG).

Nach dem Entwurf sollte die Verarbeitung von Beschäftigtendaten zugelassen sein, sofern einer der dort aufgeführten Zwecke gegeben ist. Wir haben darauf hingewiesen, dass die bisherige Regelung als weitere Zulässigkeitsvoraussetzung vorsieht, dass „dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden“ und dass ein Wegfall dieser Zulässigkeitsvoraussetzung eine materiell-rechtliche Schlechterstellung bedeuten würde. Wir haben daher die Senatorin für Finanzen gebeten, an der bisherigen Regelung festzuhalten. Die Senatorin für Finanzen hat dies zugesagt. Damit bleibt es dabei, dass die Erhebung von Beschäftigtendaten nur zulässig ist, soweit sie für die genannten Zwecke erforderlich ist und dadurch gleichzeitig schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden.

Des Weiteren haben wir auf den hohen Schutz besonderer Arten von Daten (Angaben über die ethnische und rassische Herkunft und andere) aufgrund der EU-Datenschutzrichtlinie und der entsprechenden Regelung im Bremischen Datenschutzgesetz (BremDSG) hingewiesen. Danach ist die Verarbeitung dieser Daten nur zulässig, wenn eine Rechtsvorschrift dies ausdrücklich vorsieht. Einstellungsbehörden erheben und speichern über Bewerberinnen und Bewerber regelmäßig den Geburtsort und die Staatsangehörigkeit, insoweit handelt es sich um Angaben über die ethnische und rassische Herkunft. Während die Kenntnis der Einstellungsbehörde vom Geburtsort nicht für die Einstellung in den öffentlichen Dienst erforderlich ist, ist die Staatsangehörigkeit zumindest nach dem Beamtenstatusgesetz bei der Aufnahme in das Beamtenverhältnis zwingend erforderlich, sodass wir vorgeschlagen haben, für die Verarbeitung dieses Datums eine ausdrückliche Erlaubnisnorm zu schaffen.

Die Senatorin für Finanzen vertritt dagegen die Auffassung, dass der Geburtsort im Rahmen der Identitätsprüfung der Person über die Vorlage der Geburtsurkunde erhoben wird, dieses Datum sowie die Staatsangehörigkeit keine Angaben über die ethnische oder rassische Herkunft sind und verweist hierzu unter anderem auf die Gesetzesbegründung zum Allgemeinen Gleichbehandlungsgesetz (AGG), wonach die ethnische Herkunft in einem weiten Sinne verstanden werde.

Gleichwohl halten wir es wegen der von der EU-Datenschutzrichtlinie und dem Bremischen Datenschutzgesetz ausdrücklich anerkannten und festgelegten besonderen Sensibilität dieser Daten weiterhin für erforderlich und im Übrigen für unschädlich, hierfür eine ausdrückliche Erlaubnisnorm zu schaffen.

### 10.5 Telefonverkehrsmessung im Rahmen des Projektes „Telefonisches BürgerServiceCentrum / D115“

Der Senat der Freien Hansestadt Bremen möchte seinen telefonischen Bürgerservice verbessern und damit einhergehend die Voraussetzungen für einen Beitritt Bremens zum nationalen D115-Verbund schaffen. Hinter dem Projekt D115 steckt das Ziel, Bürgerinnen und Bürgern unter einer einheitlichen Servicebehördenrufnummer eine direkte Verbindung in die Verwaltung zu bieten. Es spielt dabei keine Rolle, welche Verwaltungsebene, konkrete Behörde oder Dienststelle für das jeweilige Anliegen zuständig ist.

Im Rahmen des bundesweiten Pilotprojektes D115 haben sich bereits mehrere BürgerServiceCenter zusammengeschlossen, um festgelegte qualitative und quantitative Mindeststandards hinsichtlich der Servicezeit, Erreichbarkeit, Rückmeldefrist sowie Erledigung der Anliegen zu erbringen. Es wird erwartet, dass sich aus dem D115-Servicelevel ein einheitlicher Standard für den telefonischen Bürgerservice in Deutschland entwickeln wird.

Die Zuständigkeit für die Umsetzung von Maßnahmen zur Erfüllung dieser Standards in Bremen liegt bei der Senatorin für Finanzen. Um Informationen beispielsweise über das Telefonvolumen und den Wirkungsgrad zu erhalten, wurde die Durchführung einer Telefonverkehrsmessung geplant. Es handelt sich dabei um eine Erreichbarkeitsmessung, die von einer externen Firma durchgeführt wird. Der Inhalt der Telefongespräche wird bei den Messungen nicht aufgezeichnet. Ein Speichern der Gesprächsinhalte wäre nach dem Telekommunikationsrecht unzulässig. Die datenschutzrechtlichen Belange der in der bremischen Verwaltung Beschäftigten werden dadurch sichergestellt, dass keine einzelfallbezogenen Auswertungen der Informationen erfolgen, sondern die Daten gruppenbezogen erfasst und aufbereitet werden. Jeder Gruppe sind mindestens fünf Nebenstellenrufnummern zu-

geordnet. Dadurch kann kein Bezug zu einzelnen Mitarbeiterinnen und Mitarbeitern hergestellt werden.

Unsere Anforderungen an die technischen und organisatorischen Maßnahmen zur Durchführung der geplanten Telefonverkehrsmessung im bestehenden Telekommunikationsnetzwerk haben wir der Senatorin für Finanzen umfassend dargestellt.

Geplant war allerdings zunächst, die Telefonnummern der anrufenden Bürgerinnen und Bürger zu speichern, um herauszufinden, wie hoch die Anzahl der Wahlwiederholungen ist. Dagegen äußerten wir datenschutzrechtliche Bedenken. Bei den eingehenden Anrufen kann nicht zwischen privaten und dienstlichen Anrufen unterschieden werden, sodass es sich um Verbindungs- und Verkehrsdaten handelt, die dem Telekommunikationsgesetz (TKG) unterliegen. Nach § 88 Absatz 3 TKG dürfen diese Daten nur zur Bereitstellung des Telekommunikationsdienstes und unter speziellen Voraussetzungen, die das TKG vorgibt, verarbeitet werden. Die vorgesehene Telefonverkehrsmessung gehört nicht dazu. Wir teilten der Senatorin für Finanzen daher mit, dass eine Speicherung der Anrufernummern nur dann zulässig wäre, wenn die letzten drei Ziffern der Nummern gelöscht würden oder auf andere Weise sichergestellt werden könnte, dass ein Personenbezug nicht mehr hergestellt werden kann. Diese Lösung wurde als nicht praktikabel angesehen, da dadurch bei der Ermittlung der Wahlwiederholungen zu große Ungenauigkeiten auftreten würden. Anderweitige Verfahren, die Anzahl der Wahlwiederholungen datenschutzkonform zu ermitteln, konnten von der beauftragten Firma nicht zur Verfügung gestellt werden, sodass die Senatorin für Finanzen auf die Ermittlung der Wahlwiederholungen verzichtete. Das geplante Verfahren zur Ermittlung der Anzahl der Wahlwiederholungen wird aufgrund der datenschutzrechtlichen Unzulässigkeit in der Zwischenzeit nach Auskunft der beauftragten Firma nicht mehr angeboten.

### 10.6 Projekt „Unbarer Zahlungsverkehr“ für die Verwaltung

Wie bereits im letzten Jahr berichtet (vergleiche 31. Jahresbericht, Ziffer 9.22), ist in der gesamten bremischen Verwaltung die Möglichkeit eines unbaren Zahlungsverkehrs geplant. Seit 2007 wird dieses Projekt (früher „Bargeldloser Zahlungsverkehr für Verwarnungen“) durch uns beraten.

In diesem Berichtsjahr wurde das Sollkonzept erstellt, zu dem wir im Sommer umfassend Stellung genommen haben. Eine Beantwortung unserer Fragen ist bisher nicht erfolgt. Die Landeshauptkasse teilte auf Nachfrage mit, dass die Neuausrichtung dieses Projektes noch nicht abgeschlossen sei.

## 11. Medien

### 11.1 Veröffentlichung von amtlichen Dokumenten im Internet

In letzter Zeit erhielten wir vermehrt Eingaben, die sich gegen die Veröffentlichung amtlicher Dokumente im Internet richten. Meistens erlangten die Petentinnen und Petenten erst Kenntnis über diese Publikationsform, indem sie die zu ihrem Namen veröffentlichten Informationen über eine Suchmaschine im Internet recherchierten und dort auf die entsprechenden Dokumente stießen. Die Eingaben betrafen unter anderem die Veröffentlichung von Wahlvorschlägen mit Namen, Beruf, Geburtsort, Geburtsdatum, Adresse der Kandidaten, und Beiratsprotokollen mit Bürgeranträgen mit Angaben zu Namen, Antrag und Anschrift.

Oftmals waren die Dokumente in Druckform allgemein zugänglich. Dennoch liegt in der Veröffentlichung im Internet eine andere Qualität. Internetveröffentlichungen kommt gegenüber den Betroffenen eine ungleich höhere Eingriffsintensität zu, da die personenbezogenen Daten einfach recherchierbar und weltweit rund um die Uhr von einem unübersehbar großen Personenkreis zweckbindungsfrei, unbeschränkt und in Sekundenschnelle abrufbar sowie beliebig mit anderen Daten verknüpfbar sind. Die Ausübung der unabdingbaren datenschutzrechtlichen Rechte ist den Betroffenen faktisch nicht mehr möglich, insbesondere eine Löschung beziehungsweise Berichtigung der einmal eingestellten Daten ist aufgrund der unkontrollierbaren Vervielfältigung im Netz praktisch nicht mehr realisierbar. Zudem besteht eine erhöhte Gefahr des Missbrauchs der Identitätsdaten im Netz.

Da in der Veröffentlichung von personenbezogenen Daten im Internet und der damit einhergehenden Datenübermittlung ein Eingriff in das Grundrecht auf informatio-

nelle Selbstbestimmung der Betroffenen liegt, ist die Veröffentlichung ohne eine spezielle die Veröffentlichung erlaubende Vorschrift beziehungsweise die Einwilligung der Betroffenen nicht zulässig. Der Umstand, dass der Gesetzgeber in einigen Bereichen gesetzliche Regelungen für Internetveröffentlichungen geschaffen hat, zum Beispiel Zwangsversteigerungen, Insolvenzbekanntmachungen, spricht dafür, dass auch er von dem Erfordernis einer bereichsspezifischen Regelung ausgegangen ist. Zudem existieren oftmals Veröffentlichungsregelungen in den bereichsspezifischen Gesetzen, die gerade keine Internetveröffentlichung, sondern beispielsweise nur eine Veröffentlichung im Amtsblatt oder einer Tageszeitung vorsehen. Da es spezialgesetzliche Regelungen gibt oder eben bewusst auch nicht gibt, bleibt kein Raum für eine Anwendung der allgemeinen Landesdatenschutzgesetze und damit für eine Interessenabwägung in Bezug auf die Veröffentlichung von Daten aus allgemein zugänglichen Quellen. Selbst wenn noch eine Interessenabwägung nach den allgemeinen Datenschutzgesetzen vorgenommen würde, würden schutzwürdige Belange der Betroffenen einer Internetveröffentlichung offensichtlich entgegenstehen.

Grundsätzlich sind folgende Gesichtpunkte bei Internetveröffentlichungen durch öffentliche Stellen zu beachten:

Zunächst sollte geprüft werden, ob eine Veröffentlichung ohne Personenbezug möglich ist. Hinsichtlich der Veröffentlichung von Beiratsprotokollen haben wir mit der Senatskanzlei und den Ortsämtern beispielsweise vereinbart, dass in Beiratsprotokollen zwar Bürgeranträge mitprotokolliert, der Name aber in einem Anhang festgehalten wird. Im Protokoll steht lediglich „ein Bürger (1) beantragt“. So ist die Einstellung von Beiratsprotokollen ins Internet aus datenschutzrechtlicher Sicht unproblematisch.

Falls eine anonymisierte Veröffentlichung nicht möglich ist, sollte eine Einwilligung der Betroffenen thematisiert werden, da hierdurch die Betroffenen selbst über die Veröffentlichung ihrer personenbezogenen Daten bestimmen können. Hiermit würde ihrem Grundrecht auf informationelle Selbstbestimmung im hohen Maße Rechnung getragen.

Wenn die Einholung der Einwilligung problematisch ist, ist zu überlegen, ob eine Internetveröffentlichung wirklich erforderlich ist oder ob aufgrund der höheren Belastung für die Betroffenen nicht doch darauf verzichtet werden sollte. Auf Bundesebene wurde beispielsweise bei der Novellierung der Bundeswahlordnung (BWO) im Jahr 2008 die im ursprünglichen Entwurf vorgesehene Schaffung einer Befugnis zur – zusätzlichen – Internetveröffentlichung (§ 86 Absatz 1 Seite 2 BWO-E) aufgrund der erheblichen datenschutzrechtlichen Bedenken wieder gestrichen.

Wenn dennoch an der Veröffentlichung im Internet festgehalten werden soll, sollten bei Schaffung der gesetzlichen Grundlage unter anderem folgende Gesichtspunkte Berücksichtigung finden:

— Reduktion des Datensatzes auf das Erforderliche – Grundsatz der Datensparsamkeit –,

— Festlegung von Löschfristen,

— Regelungen zur Sicherstellung der Unversehrtheit, Vollständigkeit, Aktualität und jederzeitigen Ursprungszuordnung der Veröffentlichung,

— keine Möglichkeit eines Downloads,

— Einschränkungen in der Suchfunktion,

— keine Suchmaschinenrecherchierbarkeit.

### 11.2 Keine Verpflichtung zur Herausgabe von E-Mails ohne richterliche Anordnung

Ein Mitarbeiter einer öffentlichen Stelle hatte im Rahmen seiner dienstlichen Tätigkeit eine E-Mail an einen Veranstalter von Weiterbildungsmaßnahmen geschickt. Die E-Mail sollte Äußerungen enthalten haben, welche die öffentliche Stelle zum Anlass für eine Abmahnung nahm. Der betroffene Mitarbeiter erhob gegen die Erteilung der Abmahnung Klage bei Gericht. Im arbeitsgerichtlichen Verfahren bat das Gericht den Arbeitgeber um Vorlage der E-Mail. Da der Arbeitgeber jedoch nur mündlich über die Inhalte informiert worden war, lag ihm die E-Mail nicht vor. Er bat daraufhin den Veranstalter um Herausgabe der in Rede stehenden E-Mail.

Dieser wandte sich aufgrund datenschutzrechtlicher Bedenken an uns und bat um Beratung.

Die Bedenken des Veranstalters teilten wir im vollen Umfang und rieten ihm, die E-Mail nicht herauszugeben. In der Herausgabe hätte ein Eingriff in das Recht auf informationelle Selbstbestimmung des Betroffenen gelegen. Die Äußerungen des Betroffenen waren ausschließlich an den Veranstalter gerichtet. Der Betroffene wollte gerade nicht, dass andere von dem Inhalt Kenntnis erlangen. Das Recht auf informationelle Selbstbestimmung ist allerdings nicht schrankenlos gewährleistet. Für Eingriffe in dieses hätte es jedoch einer Rechtsgrundlage beziehungsweise der Einwilligung des Betroffenen bedurft. Von einer Einwilligung konnte offensichtlich nicht ausgegangen werden. Als Rechtgrundlage wären zum Beispiel die in § 95 Strafprozessordnung (StPO) oder in § 142 Zivilprozessordnung (ZPO) normierten Herausgabepflichten in Betracht gekommen. Ein entsprechendes Verlangen hätte aber vom Gericht geäußert werden müssen. Dieses hätte sich gegebenenfalls an den Veranstalter wenden können. Das bloße Herausgabeverlangen der öffentlichen Stelle genügt nicht datenschutzrechtlichen Anforderungen.

### 11.3 Datenerhebung beim Nachbarn durch Rundfunkgebührenbeauftragten

Bei einem Bremer Bürger klingelte ein Rundfunkgebührenbeauftragter und versuchte, ihn über seine Nachbarn auszufragen. Der Rundfunkgebührenbeauftragte wollte wissen, wie lange diese schon in der Wohnung leben würden und wie viele Personen es wären. Der Bürger erklärte dem Rundfunkgebührenbeauftragten auf diese Fragen, dass er nicht oft zu Hause sei und es nicht wisse. Da er die Vorgehensweise befremdlich fand, beschwerte er sich darüber bei uns.

Zu Recht – Daten bei Dritten dürfen nach § 10 Absatz 3 des Bremischen Datenschutzgesetzes (BremDSG) nur erhoben werden, wenn eine Rechtsvorschrift dies erlaubt oder zwingend voraussetzt oder wenn der Schutz von Leben und Gesundheit davon abhängt. Da keine Rechtsvorschrift ersichtlich ist und die anderen Voraussetzungen nicht erfüllt sind, war die Frage nach den Nachbarn datenschutzrechtlich unzulässig. Eine Auskunftsverpflichtung sieht der Rundfunkgebührenstaatsvertrag nur für die Betroffenen selbst und Personen vor, die mit den Betroffenen in häuslicher Gemeinschaft leben. Nachbarn sind hiervon nicht erfasst.

Radio Bremen, für das die Gebühreneinzugszentrale (GEZ) im Rahmen der Auftragsdatenverarbeitung tätig ist, räumte ein, dass die Befragung bei Nachbarn datenschutzrechtlich zu beanstanden sei und bedauerte den Vorfall. Der geschilderte Fall führte dazu, den Rundfunkgebührenbeauftragten einer erneuten, gesonderten Schulung zu unterziehen. Zudem entschuldigte sich die Gebiets-Rundfunkbeauftragte beim Betroffenen für das Verhalten des Mitarbeiters.

## 12. Bremerhaven

### 12.1 Themen aus Bremerhaven

An dieser Stelle werden alle Ziffern dieses Berichts aufgeführt, die sich mit Themen aus Bremerhaven beschäftigen. Sie finden sich unter Ziffer 3.1 – Workshops der behördlichen Datenschutzbeauftragten 2009, Ziffer 5.1 – Künstliche DNA, Ziffer 5.10 – Melderegisterauskünfte und Auskunftssperren, Ziffer 5.12 – Einrichtung eines automatisierten Direktzugriffs auf Melderegisterdaten für Kommunalbehörden in Bremen und Bremerhaven ohne gesetzliche Grundlage, Ziffer 7.3 – BAgIS / ARGE Job-Center Bremerhaven, Ziffer 7.13 – Bevölkerungsumfrage Gesundheit, Ziffer 12.2 – Videoüberwachung der Kassenautomaten im Sozialamt, Ziffer 13.5.2 – Bekanntgabe von Bewerberdaten innerhalb der Sparkassenorganisation, Ziffer 13.5.5 – Bewertung der Persönlichkeit von Redakteurinnen und Redakteuren, Ziffer 13.8.4 – Prüfung von Onlineshops, Ziffer 13.9.1 – Unzureichende Datenschutzvorkehrungen bei SB-Zahlungsverkehrsterminals der Sparkassen, Ziffer 13.11 – Ordnungswidrigkeitsverfahren nach dem Bundesdatenschutzgesetz.

### 12.2 Videoüberwachung der Kassenautomaten im Sozialamt

Anlässlich eines anderweitigen Termins im Sozialamt Bremerhaven fiel uns auf, dass die dortigen Kassenautomaten videoüberwacht werden. Dabei stellten wir fest, dass der gesamte Flur von der Videoüberwachung erfasst wird und somit Antragstellerinnen und Antragsteller sowie sonstige den Flur passierende Personen, wie Be-

schäftigte, Besucherinnen und Besucher und so weiter, der Überwachung ausgesetzt sind. Nach Auskunft der Stadtkasse dient die Videoüberwachung ausschließlich dazu, diese im Bedarfsfall (Vandalismus beziehungsweise Unregelmäßigkeiten beim Zahlgeschäft) als Beweissicherung heranzuziehen. Die Vorgaben des Bremischen Datenschutzgesetzes (BremDSG) zur Videoüberwachung sehen unter anderem vor, den Überwachungsbereich festzulegen. Nach einer Prüfung der Überwachungsanlage haben wir erreicht, dass die Kameras nur den Kassenautomaten und den unmittelbar davor liegenden Flurbereich erfassen und insoweit fest installiert werden. Außerdem wurden deutlich sichtbare, auf den Umstand der Überwachung hinweisende Schilder angebracht und die Speicherdauer der Aufnahmen zeitlich auf drei Tage begrenzt.

## 13. Datenschutz in der Privatwirtschaft

### 13.1 Novellierung des Bundesdatenschutzgesetzes

Ausgelöst durch die diversen Datenskandale im Jahr 2008 wurde vom Bundesministerium des Innern die Novellierung des Bundesdatenschutzgesetzes (BDSG) in Angriff genommen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte schon vor den Skandalen wiederholt auf die Missbrauchsgefahren hingewiesen, die von massenhaften Datensammlungen privater Unternehmen und ihrer unkontrollierten Nutzung ausgehen. Zuletzt im April 2008 forderte die Konferenz den Gesetzgeber zu einer grundlegenden Modernisierung und Verbesserung des Datenschutzes auf und mahnte eine neue Datenschutzkultur an (vergleiche 31. Jahresbericht, Ziffer 20.3).

Nachdem die Datenskandale überhand nahmen, wurden am 4 September 2008 auf einem Spitzentreffen im Bundesministerium des Innern, dem sogenannten Datenschutzgipfel, Sofortmaßnahmen zum Schutze der Betroffenen und die damit einhergehenden gesetzgeberischen Korrekturmaßnahmen im Bundesdatenschutzgesetz erörtert. Dennoch erschien es bis kurz vor Verabschiedung der Novelle im Juni 2009 ungewiss, ob die Änderungen des Datenschutzrechts im Bereich der privaten Wirtschaft überhaupt noch vor Ende der Legislaturperiode beschlossen werden würden. Massive Lobbyarbeit hatte dazu geführt, dass der ursprünglich deutlich datenschutzfreundlichere Gesetzentwurf verwässert wurde. Die Verwendung von Adressdaten für Werbezwecke sollte nach dem ersten Entwurf im Regelfall nur mit Einwilligung der Betroffenen rechtmäßig sein. Der Aufschrei in der Wirtschaft ließ aber befürchten, dass das ganze Gesetz an dieser Regelung scheitern würde. In dem im Juni 2009 verabschiedeten Gesetz gibt es eine Reihe von Ausnahmen für die Weitergabe von listenmäßig zusammengefassten Daten – sogenanntes Listenprivileg. Die Weitergabe ist erlaubt, wenn die Herkunft der Daten aus der jeweiligen Werbung eindeutig hervorgeht. Weitere Ausnahmen gelten für die Eigenwerbung von Unternehmen, Berufswerbung und Spendenwerbung.

Bei aller Kritik an der Abschwächung des ursprünglichen Entwurfs gibt es für Bürgerinnen und Bürger Verbesserungen:

— Marktbeherrschende Unternehmen dürfen Vertragsabschlüsse nicht von datenschutzrechtlichen Einwilligungen abhängig machen – Koppelungsverbot.

— Durch § 42 a BDSG ist eine Informationspflicht bei unrechtmäßiger Kenntniserlangung in das Gesetz aufgenommen worden. Unternehmen müssen die betroffenen Bürgerinnen und Bürger und die Datenschutzaufsichtsbehörden über schwerwiegende Datenschutzverstöße unverzüglich informieren.

— Die Datenschutzaufsichtsbehörden können höhere Bußgelder verhängen und dabei auch die Höhe des wirtschaftlichen Vorteils, der durch den Datenschutzverstoß erzielt wurde, berücksichtigen – Gewinnabschöpfung.

— Die Datenschutzaufsichtsbehörden können rechtswidrige Datenverarbeitungen untersagen – Anordnungsbefugnis.

— Die betrieblichen Datenschutzbeauftragten erhalten Kündigungsschutz und das Recht auf bezahlte Fortbildungen.

— Die Regelungen zur Auftragsdatenverarbeitung wurden konkretisiert.

Die Datenschutzskandale verletzen vorwiegend die schutzwürdigen Belange der Beschäftigten durch Arbeitgeber. Aus diesem Grunde hat sich der Bundesgesetzgeber dazu entschlossen, in § 32 Bundesdatenschutzgesetz eine bereichsspezifische

und materiell–rechtliche Regelung zum Beschäftigtendatenschutz zu schaffen. Gleichwohl kann diese Regelung – auch nach Auffassung der Bundesregierung und des Bundestages – nur als Einstieg in ausführlichere Regelungen zum Beschäftigtendatenschutzgesetzes betrachtet werden. Diese sollen nach der Vereinbarung der jetzigen Regierungskoalition innerhalb der jetzt laufenden Legislaturperiode des Deutschen Bundestages geschaffen werden (vergleiche Ziffer 13.2 dieses Berichts).

Schon lange wurden die Regelungen des Bundesdatenschutzgesetzes auch der gestiegenen Bedeutung der Auskunfteientätigkeit im Wirtschaftsverkehr und dem weitverbreiteten Einsatz der sogenannten Scoringverfahren zur Beurteilung der Kreditwürdigkeit potenzieller Geschäftspartner nicht mehr gerecht. Daten- und Verbraucherschützer hatten bereits seit langem auf den auch insoweit bestehenden dringenden gesetzgeberischen Handlungsbedarf hingewiesen. Durch die Datenschutzskandale sahen sich Bundesregierung und Bundestag nicht nur zu den geschilderten Neuregelungen im Bereich der Datenerhebung und -verwendung für Werbezwecke veranlasst – sogenannte Datenschutznovelle II, es wurden endlich auch die lange verschleppten Gesetzgebungsarbeiten (vergleiche 31. Jahresbericht, Ziffer 18.4.2) im Bereich des Auskunfteienwesens wieder forciert – sogenannte Datenschutznovelle I. Am 29. Mai 2009 nahm schließlich der Bundestag den Novellierungsentwurf der Bundesregierung (vergleiche Bundestags-Drucksachen 16/10529, 16/10581) an, am 31. Juli 2009 wurde das „Gesetz zur Änderung des Bundesdatenschutzgesetzes“ im Bundesgesetzblatt verkündet (vergleiche BGBl. I 2009, Seite 2254 ff.). Auch die neuen gesetzlichen Regelungen im Auskunfteienbereich bleiben – wohl ebenfalls aufgrund der massiven Lobbyarbeit betroffener Wirtschaftskreise – weit hinter dem zurück, was aus datenschutzrechtlicher Sicht für einen effektiven Schutz der Verbraucher notwendig gewesen wäre (Näheres hierzu unter Ziffer 13.3 dieses Jahresberichts; zur Kritik bereits im 31. Jahresbericht unter Ziffer 18.8.1).

Es bleibt zu hoffen, dass dieser mit dem Datenschutzgipfel im letzten Jahr begonnene Weg zu mehr Datenschutz im Bereich der privaten Wirtschaft konsequent weiter beschritten wird und die Novelle erst der Anfang einer grundlegenden Modernisierung des Datenschutzrechts ist. Die Datenschutzbeauftragten des Bundes und der Länder haben zu Beginn der neuen Legislaturperiode den Gesetzgeber erneut auf den Handlungsbedarf hingewiesen (vergleiche Ziffer 16.10 dieses Berichts). Die Forderungen in der Entschließung beschränken sich nicht nur auf den Datenschutz in der Privatwirtschaft, sondern haben auch die Gesetzgebung im öffentlichen Bereich im Blick. Hier ist der Gesetzgeber in den letzten Jahren oftmals mit der Schaffung von Eingriffsgrundlagen in Bürgerrechte weit über das Ziel hinausgeschossen. Eine der Forderungen ist unter anderem, die gesetzliche Ermöglichung von Vorratsdatenspeicherungen und Onlinedurchsuchungen zurückzunehmen.

Da die Novelle auch mehrere positive Ansätze enthält, die sich auf das Bremische Datenschutzgesetz (BremDSG) übertragen lassen, haben wir beim Senator für Justiz und Verfassung nachgefragt, ob eine Novellierung des Bremischen Datenschutzgesetzes geplant sei. Insbesondere wäre unseres Erachtens eine Konkretisierung der Auftragsdatenverarbeitung und die Informationspflicht bei Datenschutzpannen sinnvoll. Der Senator für Justiz und Verfassung teilte uns mit, dass er unsere Anregungen zum Anlass nehmen würde, darüber nachzudenken.

### 13.2 Neue gesetzliche Regelungen zum Beschäftigtendatenschutz aufgrund der Skandale

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits seit dem Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983 mehr oder weniger regelmäßig die Schaffung eines Arbeitnehmerdatenschutzgesetzes gefordert, zuletzt auf ihrer 73. Konferenz vom 8. bis 9. März 2007 in der Entschließung „GUTE ARBEIT in Europa nur mit gutem Datenschutz“ (vergleiche 30. Jahresbericht, Ziffer 21.5) und auf ihrer 77. Konferenz vom 26. bis 27. März 2009 (vergleiche Ziffer 16.2 dieses Berichts). Seit Erlass des Volkszählungsurteils haben sich fast alle Regierungen in ihren jeweiligen Koalitionsvereinbarungen die Verabschiedung eines Arbeitnehmerdatenschutzgesetzes vorgenommen. Die in der Öffentlichkeit bekannt gewordenen Datenmissbrauchsskandale der letzten zwei Jahre in der Wirtschaft, wie die Bespitzelung der Beschäftigten durch Detektive unter Einsatz von Videoüberwachung bei Lidl, das Beschäftigtenscreening bei der Deutschen Bahn, die Telekommunikationsüberwachung der Beschäftigten bei der Telekom und der

Deutschen Bahn und so weiter, haben gezeigt, dass immer weniger Rücksicht auf die Persönlichkeitsrechte der Beschäftigten genommen wird. Der starke öffentliche Druck auf den Bundesgesetzgeber hat dazu geführt, dass der Bundestag kurz vor Ablauf der Legislaturperiode einen neuen § 32 im Bundesdatenschutzgesetz (BDSG) geschaffen hat, der erstmals speziell den Beschäftigtendatenschutz materiell-rechtlich regelt.

Danach dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigtenverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.

Des Weiteren wird dort geregelt, dass zur Aufdeckung von Straftaten personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Im Übrigen wurde festgelegt, dass die Beteiligungsrechte der Interessenvertretungen der Beschäftigten unberührt bleiben.

Diese Regelungen stellen einen ersten Schritt in die richtige Richtung dar. Sie reichen jedoch bei Weitem nicht aus, um die Rechte der Betroffenen im Arbeitsverhältnis angemessen zu wahren. Die bisherigen Regelungen zum Datenschutz am Arbeitsplatz sind in einer Vielzahl von Gesetzen weit gestreut und unübersichtlich. Sowohl Arbeitgeber als auch Arbeitnehmer sind nach wie vor auf eine komplexe Analyse der bestehenden Rechtsprechung, insbesondere des Bundesarbeitsgerichts, angewiesen, die indes naturgemäß einzelfallbezogen ist und allenfalls von einem kleinen Expertinnen- und Expertenkreis überblickt wird.

Die jetzigen Regierungsparteien haben in ihrer Koalitionsvereinbarung für die Jahre 2009 bis 2013 festgelegt, Regelungen für Bewerberinnen oder Bewerber und Arbeitnehmerinnen oder Arbeitnehmer in einem eigenen Kapitel im Bundesdatenschutzgesetz zu schaffen. Kurz nach Amtsantritt der neuen Bundesregierung ist ein Entwurf der SPD-Bundestagsfraktion zum Datenschutz im Beschäftigungsverhältnis in den Bundestag eingebracht worden. Darüber hinaus hat die Bundestagsfraktion Bündnis 90/Die Grünen Anfang Dezember dieses Jahres den Antrag „Persönlichkeitsrechte abhängig Beschäftigter sichern – Datenschutz am Arbeitsplatz stärken“ vorgelegt und die Bundesregierung aufgefordert, noch vor der Sommerpause 2010 einen Gesetzentwurf zum Schutz der Beschäftigten vorzulegen. Es bleibt abzuwarten, ob und in welcher Weise die Datenschutzbeauftragten des Bundes und der Länder in die Gesetzesberatungen einbezogen werden.

### 13.3 Neuregelung der Auskunfteientätigkeit durch die BDSG-Novelle I

Der Datenumgang bei Auskunfteien und zwischen Auskunfteien und kreditgewährenden Stellen basierte bislang entweder auf den generalklauselartigen Abwägungstatbeständen der §§ 28 und 29 Bundesdatenschutzgesetz (BDSG) oder auf einer mehr oder weniger freiwilligen Einwilligung der Betroffenen in die Datenerhebung beziehungsweise Datenverwendung. Aufgrund der Auslegungsspielräume der Vorschriften bestand vielfach Rechtsunsicherheit hinsichtlich der Zulässigkeit bestimmter Datenerhebungen beziehungsweise -verwendungen. Insbesondere konnte auch den besonderen Risiken, die mit Scoringverfahren für Betroffene verbunden sind (ein schlechter Scorewert kann die wirtschaftliche Existenzfähigkeit gefährden) über die bestehenden Regelungen nur unzureichend begegnet werden. Schon lange hatten daher Daten- und Verbraucherschutz auf einen dringenden gesetzlichen Regelungsbedarf im Hinblick auf den Datenumgang bei Auskunfteien und insbesondere auch beim sogenannten Scoring (siehe hierzu auch unter Ziffer 13.6.4) hingewiesen. Nachdem sich bereits im März 2007 der Bundestagsinnenausschuss mit der Frage des Datenschutzes im Auskunfteienwesen befasst hatte, gelang es dem Bundestag schließlich im Sommer 2009, sich auf gesetzliche Neuregelungen in diesem Bereich zu verständigen. Das entsprechende Gesetz zur Änderung des BDSG wurde am 31. Juli 2009 im Bundesgesetzblatt verkündet und tritt am 1. April 2010 in Kraft.

Das Gesetz führt nunmehr insbesondere eine spezielle Regelung zur Zulässigkeit der Datenübermittlung an Auskunfteien (vergleiche § 28 a BDSG) sowie zum Scoring (vergleiche § 28 b BDSG) in das Bundesdatenschutzgesetz ein, ändert teilweise die bisherige Datenumgangsbefugnisnorm der Auskunfteien (vergleiche § 29 BDSG) und erweitert die Auskunfts- und Informationsrechte der Betroffenen gegenüber Auskunfteien und sonstigen verantwortlichen Stellen. Insbesondere die Erweiterung der Auskunfts- und Informationsrechte der Betroffenen ist dem Grundsatz nach zu begrüßen, führte doch die bisherige intransparente Verfahrensweise der Auskunfteien und ihrer Kundinnen und Kunden häufig dazu, dass Betroffene die Entscheidungen ihrer – potenziellen – Vertragspartnerinnen und Vertragspartner, der Auskunfteikunden, nicht oder zumindest kaum nachvollziehen konnten. Aufgrund der vorgesehenen Ausnahmen wird sich jedoch erst in der Praxis erweisen müssen, ob diese erweiterten Auskunfts- und Informationsrechte tatsächlich zu Verbesserungen für Betroffene führen.

Trotz erfreulicher punktueller Verbesserungen ist insgesamt leider festzustellen, dass der Gesetzgeber aufgrund massiver Einflussnahme aus der Wirtschaft nicht den Mut aufgebracht hat, im Auskunfteienbereich und dort insbesondere im Bereich der Scoringverfahren aus Datenschutzsicht zwingend notwendige und bereits seit langem geforderte Einschnitte vorzunehmen. Exemplarisch sei dies an der künftigen Regelung des § 28 b Ziffer 4 BDSG belegt, die nicht etwa – wie fortwährend gefordert – die Nutzung von Anschriftendaten für das Scoring ausschließt, sondern vielmehr sogar nunmehr ausdrücklich als zulässig einstuft, solange nur Betroffene hierüber vorab informiert wurden. Dieses sogenannte Geoscoring kann letztlich dazu führen, dass sich ein Wohnumfeld, in dem tatsächlich oder vermeintlich Personen mit niedrigem Einkommen wohnen, nachteilig auf den Scorewert und damit die Kreditwürdigkeit aller dort lebenden Bewohnerinnen und Bewohner auswirkt, unabhängig von der tatsächlichen Vermögenssituation der betroffenen Einzelnen. Einer „geographischen Sippenhaft“ ist die Tür geöffnet. Zudem begrenzt § 28 b BDSG nicht in der erforderlichen Klarheit den Einsatzbereich von Scoringverfahren, sodass weiterhin zu befürchten ist, dass Scoringverfahren – unzulässigerweise – auch für die Berechnung allgemeiner Vertragsrisiken herangezogen werden, was zu einer einseitigen Benachteiligung der Verbraucherseite führt, die ihrerseits über die Liquidität des jeweiligen Vertragsunternehmens bei Geschäftsabschluss regelmäßig weder Kenntnisse besitzt noch sich verschaffen kann. Auch die zum Schutz der Betroffenen dringend angemahnte Begrenzung der zentralen Auskunfteien auf branchenspezifische Auskunftssysteme mit branchenrelevanten Datensätzen wurde nicht umgesetzt.

Es besteht also weiterhin gesetzgeberischer Handlungsbedarf, um zu vermeiden, dass Betroffene diskriminiert und zu berechneten, ihrer Handlungsfähigkeit beraubten Objekten am Markt verkommen.

### 13.4 Betriebliche Beauftragte für den Datenschutz

Wie schon in den letzten Jahren, haben wir auch 2009 regelmäßig die Sitzungen des Erfahrungsaustauschkreises der Gesellschaft für Datenschutz und Datensicherheit (Erfa-Kreis) begleitet. Hier treffen sich betriebliche Datenschutzbeauftragte und tauschen sich über Probleme und aktuelle Ereignisse aus. Zentrales Thema der Erfa-Kreis-Sitzungen in diesem Jahr war die Novellierung des Bundesdatenschutzgesetzes (BDSG). Hier wurden insbesondere die Neuregelung der Datenverarbeitung im Auftrag in § 11 BDSG und die der personalisierten Werbung in § 28 BDSG diskutiert. Weiterhin stand die Datenvernichtung auf der Agenda des Erfa-Kreises.

### 13.5 Beschäftigtendatenschutz

#### 13.5.1 Erfassung von Bewerberdaten für angehende Familienhelferinnen

Durch die Eingabe einer Bewerberin sind wir auf einen Bewerbungsfragebogen eines Unternehmens hingewiesen worden, mit dem eine Vielzahl teils sehr sensibler Daten erhoben und gespeichert werden. Wir haben insbesondere Angaben zur persönlichen und familiären Situation; wie Familienstand, Zusammenleben mit dem Partner, eigene Kinder sowie deren Namen, Geburtsdaten und Geschlecht, sowie Angaben zur Nationalität, Glaubensgemeinschaft und zur gesundheitlichen Situation, zum Beispiel Art der Behinderung, psychische und sonstige Erkrankungen, bemängelt.

Das Unternehmen hat daraufhin erklärt, es vermittle Kinderbetreuerinnen in den Haushalt einer Familie. Damit eine von ihr beauftragte Familie beurteilen könne, ob die vom Unternehmen vorgeschlagene Person infrage komme, müsse sie das Umfeld dieser Person kennen. Insbesondere müsse die Familie ihre Erziehungsvorstellungen mit denen der vorgesehenen Familienhelferin abgleichen.

Das Unternehmen hat unsere Vorschläge akzeptiert und uns einen überarbeiteten Fragebogen vorgelegt, der die vorgenannten Daten nicht mehr enthält. Hinsichtlich der Gesundheitsdaten werde lediglich ein Gesundheitszeugnis beziehungsweise ärztliches Attest verlangt, das nur noch die Information enthält, dass keine gesundheitlichen Bedenken gegen den Einsatz von Familienhelferinnen bestehen. Soweit im Einzelfall für die Vermittlung in eine Familie die Information über die Nationalität oder Glaubensgemeinschaft gewünscht wird, werde dieses Datum nur mit wirksamer Einwilligung der Bewerberin erhoben.

### 13.5.2 Bekanntgabe von Bewerberdaten innerhalb der Sparkassenorganisation

Aus einem anderen Bundesland haben wir erfahren, dass dort Bewerberinnen und Bewerber bei Sparkassen und der Landesbank danach gefragt würden, ob sie bereits an einem Berufseignungstest als Bankkauffrau und Bankkaufmann (BEST) beziehungsweise einem Potenzialanalyseverfahren der Sparkassen und Landesbanken teilgenommen hätten. Gleichzeitig werde die Einwilligung der Betroffenen zur Überprüfung und zum Austausch der Daten mit der Sparkassenakademie verlangt. Zweck sei es auszuschließen, dass Wiederholungsbewerberinnen und -bewerber einen Wettbewerbsvorteil gegenüber Erstbewerberinnen und -bewerbern hätten. Nach einer Umfrage bei den Sparkassen in Bremen und Bremerhaven sowie der Bremer Landesbank haben zwei Kreditinstitute erklärt, an dem Verfahren beteiligt zu sein.

Wir haben daraufhin dargelegt, dass auch andere Kreditinstitute anderer Bundesländer mit ihren Bewerberinnen und Bewerbern diesen Test durchführen. Die beiden Kreditinstitute erklärten, sie halten es jedoch nicht für notwendig nachzufragen, ob Bewerberinnen und Bewerber bereits an diesem Test bei einem anderen Kreditinstitut teilgenommen hätten. Sie werteten nur ihre selbst durchgeführten Tests aus und ließen auch nur deren Ergebnisse in ihre Bewertung einfließen. Die Tatsache, ob eine Bewerberin oder ein Bewerber schon einmal bei einem anderen Institut diesen oder einen gleichgelagerten Test durchgeführt habe, sei für die Gesamtbewertung unbeachtlich und deshalb nicht erforderlich. Daraufhin haben die beiden Kreditinstitute erklärt, ab sofort auf die Frage nach der Teilnahme an früheren Tests zu verzichten.

### 13.5.3 Aufbewahrung von Arbeitsmedizin- und Strahlenschutzakten bei Konkurs

Wir wurden darüber informiert, dass ein Insolvenzverwalter beabsichtigt, einzelne Betriebsstätten eines sich in Insolvenz befindlichen Industrieunternehmens auf mehrere Firmen zu verteilen. Eine Vielzahl betriebs- und projektbezogener Unterlagen über Arbeitsplatzbelastungen und Gefährdungsbeurteilungen seien teilweise bei dem Sicherheitsingenieur der insolventen Firma vorhanden. Unser Informant befürchtete, dass diese Unterlagen vernichtet beziehungsweise nicht ordnungsgemäß an die neuen Firmen übergeben und aufbewahrt würden und dass auf diese Weise personenbezogene Daten unwiederbringlich gelöscht werden könnten. Dies hätte zur Folge, dass dadurch Rechtsansprüche von Beschäftigten, zum Beispiel auf Anerkennung einer Berufskrankheit oder Entschädigung aufgrund gesundheitlicher Beschwerden gegenüber der Berufsgenossenschaft, nicht mehr verwirklicht werden könnten. Des Weiteren befänden sich in den Räumen des betriebsärztlichen Dienstes Akten über arbeitsmedizinische Untersuchungen, die Befunde und alle sonstigen üblichen ärztlichen Aufzeichnungen enthielten.

Wir haben dargelegt, dass der Insolvenzverwalter nach der Insolvenzordnung in die Rechte und Pflichten des bisherigen Arbeitgebers eingetreten ist, sodass er für die Sicherung dieser Unterlagen verantwortlich ist. Demzufolge hat er über den Verbleib der teilweise bis zu 30 Jahre lang aufzubewahrenden Akten zu entscheiden und die Betroffenen darüber zu unterrichten. Er ist im Zusammenwirken mit dem bisherigen Betriebsarzt auch verpflichtet zu entscheiden, was nunmehr zu unternehmen ist. Es bietet sich an, dass von den neuen Firmen übernommene Beschäftigte gegenüber dem bisherigen Betriebsarzt einwilligen, die ärztlichen Unterla-

gen an den neuen Betriebsarzt zu übergeben. Alternativ können die Befunddaten auch an betroffene Beschäftigte zur Aufbewahrung übergeben werden. Der Informant hat zugesagt, den Insolvenzverwalter aufzufordern, die datenschutzrechtlich notwendigen Entscheidungen zu treffen.

### 13.5.4 Aufbewahrung Jahre zurückliegender Vorfälle in der Personalakte

Wir haben aufgrund einer Eingabe bei einem Unternehmen nachgefragt, zu welchen Zwecken die Unterlagen über einen mehr als fünf Jahre zurückliegenden Vorfall eines Beschäftigten immer noch in dessen Personalakte aufbewahrt werden müssen. Das Unternehmen hielt die Aufbewahrung der Unterlagen aufgrund der Rechtsprechung des Bundesarbeitsgerichts für zulässig. Daraufhin haben wir dargelegt, dass Unterlagen über Abmahnungen oder sonstige Verfehlungen von Beschäftigten zur Wahrung ihrer schutzwürdigen Interessen nicht unbegrenzt aufbewahrt werden dürfen, weil ihr oder ihm ansonsten arbeitsrechtliche Verfehlungen noch nach Jahren vorgehalten werden könnten, was die schutzwürdigen Interessen der Beschäftigten verletzt. Die Unterlagen müssen nach spätestens fünf Jahren aus der Personalakte entfernt und vernichtet werden. Das Unternehmen antwortete, es habe die entsprechenden Dokumente vernichtet und werde zukünftig die Aufbewahrungsfrist beachten.

### 13.5.5 Bewertung der Persönlichkeit von Redakteurinnen und Redakteuren

Von einem Medienunternehmen haben wir erfahren, dort werde die Persönlichkeit aller Redakteurinnen und Redakteure von der Chefredaktion bewertet. Es werde eine Vielzahl von Tätigkeits- beziehungsweise Persönlichkeitsmerkmalen – zum Beispiel Fotografieren, Schnelligkeit, Engagement, Kommunikationsfähigkeit, Organisationsfähigkeit – nach mehreren Stufen erhoben. Zweck der Bewertung sei es, die Redakteurinnen und Redakteure bei ihrer Arbeit unter Berücksichtigung ihrer Stärken und Schwächen gezielter einzusetzen. Zugriffe auf diese Daten hätten nur die Mitglieder der Chefredaktion. Die Beschäftigten seien über diese Datenverarbeitung nicht unterrichtet worden. Es habe jedoch Gerüchte gegeben, die zu einer großen Verunsicherung der Betroffenen geführt hatte.

Das Unternehmen hat auf unsere Anfrage die Bewertung der Redakteurinnen und Redakteure bestätigt. Aufgrund der hohen Belastung der Chefredaktion und anderer zahlreicher Teilaufgaben sei eine Unterrichtung der Betroffenen nicht erfolgt. Auch sei eine nach dem Bundesdatenschutzgesetz (BDSG) vorgeschriebene Vorabkontrolle für dieses Verfahren nicht durchgeführt worden. Des Weiteren hat das Unternehmen erklärt, die Bewertung ab sofort einzustellen, allen Betroffenen Einsicht in ihre Daten zu gewähren und die Daten anschließend zu löschen. Wegen der unzulässigen Datenerhebung haben wir ein Bußgeldverfahren eingeleitet.

### 13.5.6 Weitergabe von Bewerberdaten an die Bremer Arbeitsgemeinschaft für Integration und Soziales

Aufgrund der Eingabe eines beschäftigungslosen Petenten haben wir bei einem Unternehmen nachgefragt, zu welchen Zwecken dessen Bewerberdaten an die Bremer Arbeitsgemeinschaft für Integration und Soziales (BAgIS) übermittelt worden sind, nachdem ein Arbeitsverhältnis nicht zustande gekommen war. Das Unternehmen erklärte, es habe Zweifel an der Ernsthaftigkeit der Bewerbung gehabt. Es habe sich berechtigt gefühlt, die BAgIS über diese Zweifel an der Ernsthaftigkeit der Bewerbung zu informieren. Wir haben das Unternehmen darüber informiert, dass die Übermittlung der Bewerberdaten an die BAgIS eine schwere Beeinträchtigung der Vertraulichkeit von Bewerbungen darstellt und die aus diesem Grund unzulässige Datenübermittlung zu einer unzulässigen Datenspeicherung beim Empfänger führt. Eine solche Situation hat gesetzlich zur Folge, dass die Daten beim Empfänger zu löschen sind. Deshalb haben wir das Unternehmen aufgefordert, die BAgIS zu veranlassen, die unzulässig gespeicherten Bewerberdaten unverzüglich zu löschen und sich dies bestätigen zu lassen. Dem ist das Unternehmen inzwischen gefolgt.

### 13.5.7 Erhebung und Speicherung von Diagnosedaten über Beschäftigte beim Mercedes-Werk Bremen

Im Frühjahr 2009 hat Radio Bremen uns darüber unterrichtet, der Sender habe von Unbekannt eine CD über Diagnosedaten enthaltene Mitarbeiterlisten aus dem Mercedes-Werk Bremen erhalten. Dabei handelte es sich um Tabellen, in denen

Abteilung, Krankheitsdauer und Krankheitsgründe, also auch Diagnosen, festgehalten wurden. Die Listen datierten aus den Jahren 2006 bis 2008. Nach ersten Informationen hätten die Vorgesetzten die Beschäftigten in sogenannten Rückkehrgesprächen nach den Gründen gefragt; die Diagnosen seien dann in die Listen eingetragen worden.

Wir haben Radio Bremen gegenüber erklärt, es handele sich um einen gravierenden Verstoß gegen Datenschutzbestimmungen, sollten im Mercedes-Werk Bremen tatsächlich Diagnosedaten über Beschäftigte erhoben und gespeichert werden. Bei Vorsatz oder Fahrlässigkeit ist dies eine Ordnungswidrigkeit, die nach dem damals geltenden Bundesdatenschutzgesetz (BDSG) mit einer Geldbuße von bis zu 250.000 Euro geahndet werden kann. Nach dem neuen Bundesdatenschutzgesetz ab dem 1. September 2009 beträgt die Höchstgeldbuße 300.000 Euro. Wir haben den Fall an die zuständige Datenschutzaufsichtsbehörde für den nicht öffentlichen Bereich in Baden-Württemberg abgegeben, weil sich der Hauptsitz von Mercedes dort befindet und von dort aus das Gesundheitsmanagement zentral organisiert ist. Die dortige Aufsichtsbehörde hatte zu prüfen, ob der Konzern fahrlässig oder gar vorsätzlich gehandelt hat. Zeigt sich das Unternehmen einsichtig, entschuldigt sich und trifft Maßnahmen, damit sich ein solcher Verstoß nicht wiederholen kann, kann die Aufsichtsbehörde von dem Bußgeld absehen. Letztendlich ist gegen Mercedes in dieser Sache kein Bußgeldverfahren eingeleitet worden.

Wir haben des Weiteren auch überregionalen Medien- und Presseorganen auf Anfragen dargelegt, dass Unternehmen und Behörden nach § 84 Sozialgesetzbuch (SGB) IX ein sogenanntes Betriebliches Eingliederungsmanagement einsetzen müssen. Dabei geht es im Wesentlichen um die Reduzierung krankheitsbedingter Fehlzeiten. Untersuchungen zeigen, dass bis zu 40 Prozent der Erkrankungen berufsbedingt sind und mit den Arbeitsbedingungen zusammenhängen. Das rechtfertigt die Arbeitgeberin oder den Arbeitgeber aber nicht, Diagnosedaten zu erfragen und zu speichern. Diese Daten müssen die Beschäftigten nicht preisgeben.

## 13.6 Auskunfteien

### 13.6.1 Eingaben im Bereich der Handels- und Wirtschaftsauskunfteien

Auch im Berichtsjahr erhielten wir wieder zahlreiche Eingaben, die die Verarbeitung personenbezogener Daten durch die Handels- und Wirtschaftsauskunfteien betrafen. Erneut ging es dabei insbesondere um Themen wie die Unrichtigkeit der von den Auskunfteien verarbeiteten Daten, die Nichterteilung oder die nicht vollständige Erteilung von Auskünften oder die Überschreitung der zulässigen Speicherdauer. Erst durch unser Tätigwerden konnte erreicht werden, dass die gespeicherten Daten berichtigt oder gelöscht wurden oder aber der Auskunftsanspruch des Betroffenen durchgesetzt wurde.

In einem der Fälle beklagte sich ein Bürger, dass trotz seiner mehrfachen Aufforderungen die Auskunftei nicht bereit sei, ihm mitzuteilen, an wen die über ihn gespeicherten Daten übermittelt worden seien. Die Auskunftei habe ihm lediglich mitgeteilt, dass keine Anfrage zu seiner Person bei ihr eingegangen sei. Er sei sich allerdings sicher, dass ihn betreffende Daten an Dritte übermittelt worden sind.

Unsere Überprüfung des Vorgangs ergab, dass zu unserem Petenten tatsächlich keine Anfrage bei der Auskunftei eingegangen war. Gleichwohl waren in zwei Fällen Daten über den Betroffenen von der Auskunftei an deren Kunden übermittelt worden. Die Auskunftei begründete ihr Verhalten, gegenüber dem Petenten die Datenübermittlungen nicht zu beauskunften damit, dass die Übermittlungen aufgrund von Anfragen zu dem Unternehmen, bei dem er in unternehmensleitender Stellung tätig ist, erfolgten. Hinsichtlich der Berechtigung, bei solchen Anfragen auch die Daten von Mitarbeiterinnen und Mitarbeitern in dieser Position zu übermitteln, verwies die Auskunftei auf höchstrichterliche Rechtsprechung, die die Übermittlung auch dieser Daten im Hinblick auf eine sorgfältige Bonitätsprüfung zulasse.

Die Berechtigung, bei der Beantwortung von Anfragen zu Unternehmen auch Angaben zu dessen leitenden Personen zu übermitteln, darf nicht den Auskunftsanspruch des Betroffenen nach § 34 Bundesdatenschutzgesetz (BDSG) unbeachtet lassen. Der Anspruch auf Mitteilung, an wen die Daten des Betroffenen weitergegeben worden sind, ist umfassend und bezieht sich auf alle Datenübermittlungen, auch die, bei denen die Daten zu einem Dritten, in diesem Fall einem Unternehmen, gespei-

chert sind. Er beschränkt sich nicht auf die Datenübermittlungen, bei denen eine Anfrage direkt zu der Person des Betroffenen vorliegt.

Wir haben der Auskunftei unsere Rechtsauffassung mitgeteilt und sie aufgefordert, bei der Erteilung von Auskünften an den Betroffenen künftig auch derartige Übermittlungen einzubeziehen. Eine Antwort hierauf steht noch aus.

### 13.6.2 Schufa-Abfrage trotz Kostenübernahmeerklärung

Im Frühjahr dieses Jahres beschwerte sich ein Bürger bei uns, der sich bei einer Wohnungsgesellschaft um eine Wohnung bemüht hatte, dass trotz der Vorlage einer Kostenübernahmeerklärung eine Schufa-Auskunft über ihn eingeholt und ihm daraufhin eine Wohnung verwehrt worden sei.

Nachdem wir uns mit der Vermieterin in Verbindung gesetzt hatten, teilte diese mit, die Schufa-Auskunft würde aufgrund einer Einwilligung durchgeführt, die auf dem sogenannten Interessentenbogen für Mieter vom Mietinteressenten erteilt wurde. Da diese Einwilligungserklärung nicht den gesetzlichen Anforderungen des Bundesdatenschutzgesetzes (BDSG) entsprach, wurde die weitere Vorgehensweise in diesem Fall in einem persönlichen Gespräch mit der Gesellschaft geklärt. Daraufhin wurde aus dem Interessentenbogen für Mieter die Einwilligungserklärung über die Auskunftseinholung bei der SCHUFA entfernt und durch eine Unterrichtung ersetzt. Hiernach darf diese Auskunft nur noch in begründeten Einzelfällen, wenn es erforderlich ist, eingeholt werden. Die Mitarbeiterinnen und Mitarbeiter der Vermieterin seien durch ein Rundschreiben und eine Schulung darüber informiert worden, dass eine Schufa-Auskunft nur in begründeten Fällen nach einer Einzelprüfung zulässig ist, wenn die erteilten Auskünfte der zukünftigen Mieter nicht ausreichend sind.

### 13.6.3 Auskunftsbitte einer Auskunftei gegenüber Gewerbetreibenden

Ein Petent beschwerte sich im Berichtsjahr über eine Wirtschaftsauskunftei, die unter anderem auch Einzelgewerbetreibende anschrieb und diese aufforderte, einen dem Anschreiben beigefügten Bogen mit den im Auskunfteidatenbestand vorhandenen Daten zur Wirtschafts- und Finanzsituation des jeweiligen Gewerbetreibenden zu vervollständigen beziehungsweise zu aktualisieren. In ihrem Anschreiben wies die Auskunftei unter anderem darauf hin, dass man von der Richtigkeit der mitgeteilten Daten ausgehe, wenn man von dem Angeschriebenen binnen einer bestimmten Frist keine gegenteilige Information erhalte.

Diese Aufforderung zur Mitteilung von Wirtschafts- und Finanzdaten gegenüber Einzelgewerbetreibenden stellt eine Beschaffung personenbezogener Daten, mithin einen datenschutzrechtlich relevanten Datenerhebungsvorgang im Sinne des § 3 Absatz 3 Bundesdatenschutzgesetz (BDSG) dar. Daher waren die Vorschriften des Bundesdatenschutzgesetzes anwendbar. Für direkte Datenerhebungen bei Betroffenen schreibt das BDSG vor, dass diese insbesondere auch über die Zweckbestimmungen der Datenerhebung sowie grundsätzlich über die Empfängerkategorien zu unterrichten sind. Diese Unterrichtung muss vollständig, inhaltlich hinreichend konkret und verständlich sein. Des Weiteren müssen die Betroffenen, sofern die Datenangabe nicht gesetzlich vorgesehen, sondern wie hier, freiwillig ist, unmissverständlich auf die Freiwilligkeit ihrer Angaben hingewiesen werden. Insbesondere darf nicht der Eindruck erweckt werden, das Unterlassen der Datenauskunft führe zu Rechtsnachteilen oder die Betroffenen trügen für die Richtigkeit der gespeicherten Daten die Verantwortung. Verantwortlich für die Richtigkeit gespeicherter Daten ist nach den gesetzlichen Regelungen immer die speichernde Stelle selbst.

Das Anschreiben der Wirtschaftsauskunftei trug diesen gesetzlichen Anforderungen nicht Rechnung. Auf unsere Beanstandung hin reagierte das Unternehmen umgehend und änderte sein Anschreiben entsprechend den dargestellten gesetzlichen Vorgaben ab.

### 13.6.4 Scoring durch Auskunfteien – das vermeintliche Zaubermittel zur Reduzierung unternehmerischer Vertragsrisiken

Zur Abschätzung des finanziellen Ausfallrisikos ihrer möglichen Geschäftspartner versuchen Unternehmen im Vorfeld eines Geschäftsabschlusses immer häufiger, Informationen über deren Wirtschafts- und Finanzsituation einzuholen. Sie wenden sich zu diesem Zweck zumeist an Auskunfteien oder „Warndateien“. Diese Auskunfteien oder „Warndateien“ sammeln auf Vorrat aus unterschiedlichsten Quellen

Bonitätsinformationen und übermitteln diese gegen Entgelt an anfragende Personen oder Unternehmen. Während Handels- und Wirtschaftsauskunfteien in erster Linie Informationen über die Wirtschaftstätigkeit und Wirtschaftssituation von Unternehmen und sonst gewerblich Tätigen bereithalten, sind Verbraucherauskunfteien auf die Sammlung von Bonitätsinformationen über Verbraucherinnen und Verbraucher spezialisiert. Nach Schätzungen der Verbraucherzentrale Bundesverband e. V. dürften sich derzeit bereits weit über 100 Unternehmen in dem lukrativen Geschäftsfeld des Beauskunftens von Verbraucherbonitätsdaten bewegen, Tendenz steigend.

Die Dienste der Verbraucherauskunfteien wurden ursprünglich vor allem von Kreditinstituten, Versandhandels- sowie Telekommunikationsunternehmen in Anspruch genommen. Auf diesem Wege sollten die Gefahren, die mit einer Vorleistung verbunden sind, minimiert werden. Mittlerweile gehen jedoch teils auch weitere Branchen, etwa die Versicherungs- oder Wohnungswirtschaft, dazu über, Informationen über die Zahlungsfähigkeit und Zahlungswilligkeit ihrer potenziellen Vertragspartnerinnen oder Vertragspartner bei Auskunfteien einzuholen.

Neben den Bonitätsinformationen bieten die Auskunfteien häufig auch einen sogenannten Scorewert an. Hierbei handelt es sich um einen Wahrscheinlichkeitswert, der aus den bei den Auskunfteien vorhandenen Daten in einem mathematisch-statistischen Verfahren errechnet wird und eine Aussage über das künftige Zahlungsverhalten und damit die Kreditwürdigkeit enthalten soll. Diese Scorewerte sind für die abfragenden Stellen durchaus von Interesse, liefern sie doch eine scheinbar objektive (Zahlen-)Grundlage für Bonitätsbeurteilungen und nehmen den verantwortlichen Sachbearbeiterinnen oder Sachbearbeitern einen Teil der eigenen Entscheidungsverantwortung ab. In der Praxis entscheidet der Scorewert dann häufig nicht nur darüber, ob überhaupt Kredit gewährt wird, sondern auch, zu welchen Bedingungen.

Aus vielerlei Gründen bestehen gegen die derzeit üblichen Scoringverfahren jedoch erhebliche datenschutzrechtliche Bedenken. Nicht zuletzt gibt das verwendete Datenmaterial sowie die völlige Intransparenz des Einsatzes wie auch der Durchführung der Berechnungsverfahren Anlass zur Sorge. Die Betroffenen wissen oftmals bereits nicht, dass überhaupt Scoringverfahren zur Beurteilung ihrer Zahlungsfähigkeit und Zahlungswilligkeit verwendet wurden, sie wissen des Weiteren nicht, welche Daten mit welcher Gewichtung in das Berechnungsverfahren eingeflossen sind. Auch den Auskunfteikundinnen und Auskunfteikunden fehlt dieses Wissen regelmäßig, sodass auch sie die Werthaltigkeit des an sie übermittelten Scorewertes nicht im Mindesten beurteilen können. Schließlich bestehen auch an der tatsächlichen wissenschaftlichen Eignung der derzeit eingesetzten, von Auskunftei zu Auskunftei unterschiedlichen Berechnungsverfahren zur Vorhersage einer individuellen Ausfallwahrscheinlichkeit aufgrund der bisherigen Erfahrungen aus Praxistests massive Zweifel.

Eine im Auftrag des Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz in Auftrag gegebene und im vergangenen August vorgelegte Untersuchung der Scoringverfahren kommt dann auch zu dem Ergebnis, dass viele der bei den in die Untersuchung einbezogenen Auskunfteien, wie Arvato Infoscore, Creditreform, Bürgel, SCHUFA, gespeicherten und in die Scoreberechnung einfließenden Daten über Verbraucherinnen und Verbraucher fehlerhaft sind (vergleiche auch Frankfurter Allgemeine Zeitung in der Ausgabe vom 20. August 2009, Seite 11). Letztlich sei das Zustandekommen übermittelter Bonitätswerte nicht nachvollziehbar und ihre Aussagekraft äußerst zweifelhaft, so das Fazit der Untersuchung. Schon eine im Jahr 2008 vorgelegte, im Auftrag der Verbraucherzentrale Bundesverband e. V. durchgeführte umfangreiche Studie – abrufbar im Internet unter: http://www.vzbv.de/mediapics/scoring_studie_15_01_2008.pdf – bescheinigte dem Scoring, dass es für eine valide Bonitätsbeurteilung der Verbraucherinnen und Verbraucher in der Praxis kaum tauglich sei. Es bleibt zu hoffen, dass diese Erkenntnis allmählich auch ins Bewusstsein der Auskunfteikundinnen und Auskunfteikunden dringt.

Als Reaktion auf die bislang unzulänglichen gesetzlichen Regelungen zur Auskunfteientätigkeit und insbesondere auch zum Scoring beschloss der Bundestag im vergangenen Jahr nach zähem Ringen unter erheblicher Einflussnahme der betroffenen Wirtschaftskreise eine Novellierung des Bundesdatenschutzgesetzes, die ab 1. April 2010 in Kraft tritt (vergleiche Ziffer 13.1 dieses Berichts). In einigen Punk-

ten stärken die neuen Regelungen zwar die Rechtsstellung der Verbraucherinnen und Verbraucher gegenüber den Auskunfteien, insgesamt jedoch bleiben die Neuregelungen weit hinter dem zurück, was für einen effektiven Schutz des informationellen Selbstbestimmungsrechts der Bürgerinnen und Bürger im Zusammenhang mit der Tätigkeit der Auskunfteien erforderlich ist. Es bleibt daher zu befürchten, dass die Tätigkeit der Auskunfteien, die auch immer wieder Gegenstand unserer Tätigkeitsberichte in den letzten Jahren war, die Datenschutzaufsichtsbehörden weiterhin in nennenswertem Umfang beschäftigen wird.

## 13.7 Gesundheit / Soziales

### 13.7.1 Datenschutzprobleme bei niedergelassenen Ärztinnen und Ärzten

Im Jahr 2009 war ein deutlicher Anstieg der Beschwerden über mangelnde Sensibilität im Umgang mit Patientendaten und der Missachtung von Betroffenenrechten in Arztpraxen zu verzeichnen. Da Beschwerden ähnlichen Inhalts in geringerer Anzahl auch in den vorangegangenen Jahren geäußert wurden, gehen wir nicht davon aus, dass sich die datenschutzrechtliche Situation in Arztpraxen insgesamt verschlechtert hat, sondern dass die Patientinnen und Patienten insgesamt sensibler in Bezug auf Datenschutzfragen reagieren.

In verschiedenen Fällen erreichten uns Beschwerden über die Verweigerung der Auskunftserteilung über die bei der Ärztin oder beim Arzt gespeicherten Patientendaten. Grundsätzlich haben Betroffene nach § 34 Absatz 1 Satz 1 Nummer 1 Bundesdatenschutzgesetz (BDSG) ein Auskunftsrecht in Bezug auf die zu ihrer Person gespeicherten Daten. § 10 Absatz 2 Satz 2 der Berufsordnung für Ärzte im Land Bremen verpflichtet Ärztinnen und Ärzte, ihren Patientinnen und Patienten auf Verlangen Kopien der Unterlagen gegen Erstattung der Kosten zur Verfügung zu stellen. In einem Fall, in dem ein Patient eines Nervenarztes eine Falschdiagnose vermutete, wurde diesem die Einsicht in seine Patientenunterlagen mit der Begründung verweigert, dass die handschriftlichen Notizen schlecht zu entziffern seien, eigene subjektive Bemerkungen zur gefühlsmäßigen Reaktion auf den Patienten sowie Verdachtsdiagnosen enthalten wären, die ohne weitere Interpretation zu Missverständnissen führen und eine verletzende Wirkung haben könnten. Dadurch sah der Arzt die Gefahr, dass sich der Gesundheitszustand des Patienten verschlechtern oder es zu einer aggressiven Reaktion gegenüber dem Arzt kommen könnte. Die Rechtsprechung gesteht Ärztinnen und Ärzten im Rahmen der psychiatrischen Krankenbehandlung zu, die Einsicht in ärztliche Aufzeichnungen subjektiv wertender Art, wie beispielsweise persönliche Eindrücke bei Gesprächen oder Motive für getroffene Entscheidungen, zu verweigern, wenn dem therapeutische oder sonstige schützenswerte Interessen entgegenstehen. Diese Entscheidung hat der Arzt selbst unter Würdigung des Rechts auf Unterrichtung der Patientinnen und Patienten sowie der im Einzelfall entgegenstehenden Interessen zu treffen. Diesem Arzt haben wir aufgegeben, die Möglichkeit zu prüfen, dem Patienten eine ärztlich begleitete Einsichtnahme in die objektiven Befunde und Behandlungsfakten, wie Diagnosen, Anamnese, Medikation und so weiter, zu gewähren. Er hat dem Patienten schließlich eine um subjektive Einschätzungen bereinigte Abschrift seiner Karteikarte zur Verfügung gestellt.

In einem anderen Fall erreichte uns eine Eingabe, in der sich eine Patientin beschwerte, dass ihre Psychiaterin im Verlauf der mehrjährigen Behandlung verschiedenen unbefugten Dritten Details über ihre Erkrankung und die Behandlung mitgeteilt habe. So habe die Ärztin ihrem Ehemann, der Chefarzt einer Klinik ist, bei einem Restaurantbesuch im Biergarten Einzelheiten über die Erkrankung und Behandlung der Patientin mitgeteilt. Zudem habe die Ärztin, die zufällig bei dem gleichen Gynäkologen in Behandlung war wie ihre Patientin, sich mit diesem über deren gynäkologische Erkrankung ausgetauscht. Ferner habe die Ärztin der Patientin Details aus der Behandlung von deren Arbeitskollegin erzählt. Die Patientin teilte mit, dass ihre Ärztin sich, als sie von ihr auf den mit der Weitergabe dieser Informationen erfolgten Vertrauensbruch hingewiesen wurde, mehrfach entschuldigt habe. Uns gegenüber stritt die Ärztin dann jedoch die in allen Fällen erfolgten Offenbarungen von Patientendaten ab. Der Sachverhalt konnte deshalb von uns nicht hinreichend aufgeklärt werden. Später wurde jedoch vom Gynäkologen ein Austausch über die gemeinsame Patientin bestätigt. Da die Betroffene Strafanzeige wegen der Verletzung von Privatgeheimnissen nach § 203 Absatz 1 Strafgesetzbuch erstattet hatte, wurde unsererseits zunächst von weiteren Maßnahmen abgesehen.

In einem weiteren Fall wandte sich ein Patient an uns, der bei einem Besuch in einer Arztpraxis gesehen hatte, dass aus Anlass von technischen Problemen ein Rechner mit Patientendaten von einer Wartungsfirma abgeholt worden war. Auf seine Frage, ob die Mitarbeiter dieser Firma nun seine Patientendaten sehen und kopieren könnten, war ihm in der Praxis mitgeteilt worden, dass dies theoretisch zwar möglich sei, die Firma daran aber wohl kein Interesse haben werde. Diese Praxis ist unter Hinweis auf die ärztliche Schweigepflicht von uns aufgefordert worden, zukünftig bei der Beauftragung einer Wartungsfirma besondere Sicherungs- und Schutzmaßnahmen zu treffen, um die Veränderung, Vernichtung und unrechtmäßige Verwendung der Patientendaten durch diese zu verhindern.

Eine privat versicherte Patientin monierte, dass ihre Patientendaten vom behandelnden Arzt ohne ihre Einwilligung an ein Abrechnungsunternehmen weitergegeben wurden. Die Patientin war zwar zuvor zur Unterzeichnung einer entsprechenden Einwilligungserklärung aufgefordert worden, hatte dies jedoch nicht getan. Die Datenübermittlung erfolgte damit ohne Rechtsgrundlage und war also unzulässig. Der Arzt hat dazu mitgeteilt, dass vor der Übermittlung versäumt worden sei, das Vorliegen der Einwilligung zu prüfen. Er habe seine Mitarbeiterinnen und Mitarbeiter entsprechend informiert, um dies für die Zukunft möglichst auszuschließen.

Mehrfach haben sich Bürgerinnen und Bürger bei uns gemeldet, die von Ärztinnen oder Ärzten fehlgeleitete Telefaxe mit Patientenunterlagen erhalten haben, die an mitbehandelnde Ärztinnen oder Ärzte versandt werden sollten. Grund für solche Vorkommnisse sind regelmäßig fehlerhafte Eingaben der Faxnummer in der versendenden Arztpraxis. In den entsprechenden Fällen sind die Ärztinnen oder Ärzte von uns aufgefordert worden, die betreffenden Patientinnen und Patienten über die Vorfälle zu informieren und die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um entsprechende Falscheingaben zukünftig zu verhindern, wie beispielsweise die Nutzung einprogrammierter Faxnummern, eine Prüfung der Faxnummer durch eine zweite Person und so weiter.

Immer wieder erreichen uns Beschwerden über mangelnde Vertraulichkeit der Gespräche in Arztpraxen. Dies betrifft sowohl die Situation am Empfang als auch die Gespräche im Rahmen der ärztlichen Behandlung. Auch diese Praxen werden von uns regelmäßig dazu aufgefordert, technische und organisatorische Maßnahmen zu treffen, um zu verhindern, dass Gespräche zwischen Ärztinnen und Ärzten, deren Mitarbeiterinnen und Mitarbeitern und Patientinnen und Patienten von unbefugten Dritten mit angehört werden können. Entsprechende Maßnahmen können beispielsweise eine Sensibilisierung der Mitarbeiterinnen und Mitarbeiter, räumliche Umgestaltungen und so weiter sein.

Eine Patientin wandte sich an uns, weil ihre Ärztin – wie sie vermutete – aus Gründen der „Kundenorientierung“ alles Wissenswerte über sie, auch über die medizinischen Gegebenheiten hinaus, speicherte. So wurde beispielsweise vermerkt, dass die Patientin auf eine Nachricht auf ihrem Anrufbeantworter besorgt reagiert habe oder dass sie sich einmal darüber beschwert haben solle, als sie ihre Ärztin nicht persönlich telefonisch sprechen konnte. Auf diese Vorfälle wurde die Patientin dann regelmäßig bei späteren Arztbesuchen nach einem Blick in die EDV angesprochen. Dies gab ihr das unangenehme Gefühl, gescannt zu werden. Als sich bei einem Besuch in der Praxis dann eine ärztliche Frage ergab, die dazu führte, dass die Patientin eine sehr private Auskunft erteilte, befürchtete die Patientin, dass ihre Ärztin diese Auskunft in der elektronischen Patientenakte abspeichern würde. Sie erkundigte sich, welche Daten ihre Ärztin über sie speichern dürfe und ob sie einen Anspruch auf Löschung unzulässig gespeicherter Daten habe. Wir teilten der Betroffenen mit, dass die Ärztinnen und Ärzte die zum Zweck der Erfüllung des Behandlungsvertrages erforderlichen Daten nach § 28 Absatz 1 Bundesdatenschutzgesetz (BDSG) erheben und speichern dürfen. Darüber hinausgehende Informationen, die für die medizinische Behandlung oder Beratung nicht erforderlich sind, dürfen nur gespeichert werden, soweit dies zur Wahrung berechtigter Interessen der Ärztinnen und Ärzte erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Das bedeutet, dass für jede gespeicherte Information eine Abwägung des Interesses der Ärztin an der Speicherung mit dem Interesse der Patientin an dem Ausschluss der Verarbeitung durchzuführen war. Das Ergebnis dieser Abwägung hängt wesentlich von der Sensibilität der gespeicherten Daten und dem Zweck der Speicherung ab. Ein Anspruch auf Löschung dieser „zusätzlichen“ ge-

speicherten Daten besteht nach § 35 Absatz 5 BDSG jedenfalls dann, wenn die Patientin der Speicherung widerspricht und ihr schutzwürdiges Interesse wegen ihrer besonderen persönlichen Situation das Interesse der Ärztin an der Speicherung überwiegt.

### 13.7.2 Mangelndes Datenschutzbewusstsein bei SGB-II-Maßnahmeträgern

Im letzten Jahr wandten sich vermehrt Bezieherinnen und Bezieher von Leistungen nach dem Sozialgesetzbuch (SGB) II beziehungsweise SGB III an uns, die von der Bremer Arbeitsgemeinschaft für Integration und Soziales (BAgIS) oder der Agentur für Arbeit Bremen zur Teilnahme an Maßnahmen bei privaten Maßnahme- und Bildungsträgern verpflichtet wurden. Die eingegangenen Petitionen haben den Eindruck entstehen lassen, dass bei den beauftragten Maßnahmeträgern oft sehr unzureichendes Bewusstsein für den rechtmäßigen Umgang mit den zumeist hoch sensiblen Daten der Teilnehmerinnen und Teilnehmer vorhanden ist. Problematisch ist dabei, dass die Betroffenen die Maßnahmen nicht selbstständig beenden können, ohne Sanktionen vom zuständigen Sozialleistungsträger befürchten zu müssen und sich insofern Situationen, in denen sie häufig zu Recht ihre Rechte als verletzt ansehen, nicht ausweichen können.

Beispielsweise wandte sich ein Betroffener an uns, der von der BAgIS zur Teilnahme an einer sechsmonatigen Maßnahme bei einem Maßnahmeträger verpflichtet wurde, in deren Rahmen eine Bewertung seiner Persönlichkeit durch andere Kursteilnehmer stattfand und ein Bewerbungstraining durchgeführt wurde. Der Petent fühlte sich erheblich in seinem Persönlichkeitsrecht beeinträchtigt. Seine Frage, was mit vor Ort erstellten Bewertungsunterlagen passiere, wofür sie verwendet und wo sie verbleiben würden, wurde damit beantwortet, dass die Unterlagen bei der Kursleiterin verbleiben würden. Unsere Nachfrage ergab, dass Unterlagen der Persönlichkeitstests dazu verwendet wurden, Berichte für die BAgIS zu verfassen und dass sie für zwei Jahre aufbewahrt würden. Wir teilten dem Betroffenen mit, dass die Verpflichtung von Hilfeempfängerinnen und Hilfeempfängern zur Durchführung von Persönlichkeitstests bei privaten Maßnahmeträgern und die Übermittlung der Ergebnisse an die BAgIS keinen Verstoß gegen datenschutzrechtliche Vorschriften darstellt, weil es Rechtsgrundlagen gibt, die diese Maßnahmen zulassen. Nach § 61 Absatz 2 SGB II sind die Teilnehmerinnen und Teilnehmer einer Eingliederungsmaßnahme verpflichtet, eine Beurteilung ihrer Leistungen und ihres Verhaltens durch den Maßnahmeträger gegenüber der BAgIS zuzulassen. Gleichwohl ließ der Maßnahmeträger datenschutzrechtliche Sensibilität vermissen. Die im Seminar erstellten Bewerbungsunterlagen, wie Anschreiben, Lebensläufe, Dokumentationen über Vorstellungsgespräche, wurden für die Dauer des Seminars in einem Ordner im Seminarraum aufbewahrt und in Dateiform auf Disketten abgespeichert. Die Unterlagen waren für alle Teilnehmerinnen und Teilnehmer während der Dauer des Seminars frei zugänglich, der Zugriff auf Daten Dritter war den Teilnehmenden jedoch untersagt worden. Wir konnten erreichen, dass die Unterlagen mit den Bewerberdaten in einem verschlossenen Schrank aufbewahrt werden, sodass sie dem unkontrollierten Zugriff durch die Teilnehmerinnen und Teilnehmer entzogen sind. Weiterhin konnten wir erreichen, dass die Frist zur Aufbewahrung der Unterlagen zu den Persönlichkeitstests von zwei Jahre auf sechs Monate verkürzt wurde.

In einem anderen Fall meldete sich ein Kunde der BAgIS und teilte mit, dass er durch eine Eingliederungsvereinbarung dazu verpflichtet worden sei, an einer Informationsveranstaltung bei einem Maßnahmeträger teilzunehmen. Bei dieser Gruppenveranstaltung wurden ungefähr 15 Teilnehmerinnen und Teilnehmer über die angebotene Maßnahme, ein Praktikum, informiert. Während der Veranstaltung bemerkte der Betroffene, dass jemand im Raum ohne weitere Erklärungen Bildaufnahmen machte. Er nahm an, dass es sich um einen Reporter handelte, protestierte vehement, rief die Polizei und verließ anschließend die Veranstaltung. Unsere Nachfrage ergab, dass die Bildaufnahmen von einem Mitarbeiter des Maßnahmeträgers zum Zweck der Dokumentation und Information über das Projekt angefertigt wurden. Die Fotos, auf denen der Betroffene zu sehen war, wurden unmittelbar nach dem Vorfall gelöscht. Von den anderen Teilnehmerinnen und Teilnehmern holte sich der Maßnahmeträger eine Genehmigung zur Verwendung der Aufnahmen ein. Aufgrund unseres Hinweises, dass die Anfertigung von Bildaufnahmen ohne Einwilligung der Betroffenen eine unzulässige Datenerhebung darstellt, löschte der Maßnahmeträger schließlich auch die anderen Bildaufnahmen. Er teilte mit, zukünftig vor der Anfertigung von Bildaufnahmen die Einwilligung der Betroffenen

einzuholen. Ein entsprechendes Einwilligungsformular beabsichtigt er, mit uns abzustimmen.

### 13.7.3 Datenverarbeitung zum Zweck der Biografiearbeit in Pflegeheimen

Uns erreichten verschiedene Beschwerden von Bürgerinnen und Bürgern in Bezug auf die Datenerhebung und Datenspeicherung anhand sogenannter Biografiefragebögen in Pflegeheimen. Unsere Nachfrage ergab jeweils, dass in den Pflegeheimen für Demenzkranke Sammlungen mit biografischen Daten angelegt werden. Dafür werden über die Bewohnerinnen und Bewohner und deren Familienmitglieder teilweise sehr sensible Daten, wie zum Beispiel Daten über religiöse Überzeugungen, Krankheiten, Ängste, prägende Lebensereignisse, wie Krieg, Verlust von Angehörigen, persönliche Vorlieben und so weiter, erhoben, zum Teil, ohne dass dafür Einwilligungserklärungen der Betroffenen eingeholt werden. Die Daten werden zum Teil allen beschäftigten Pflegekräften zugänglich gemacht, um diese bei der sozialen Betreuung der Bewohnerinnen und Bewohner zu unterstützen. Die Pflegeheime teilten mit, dass dies erforderlich sei, da die Qualität der sozialen Betreuung der demenzkranken Pflegebedürftigen vom Medizinischen Dienst der Krankenkassen unter Einbeziehung biografischer Daten überprüft werde. Eine spezielle Rechtsvorschrift, die diese Datenerhebung erlaubt, gibt es nicht. Wir sind daher der Auffassung, dass die Erhebung der biografischen Daten der Bewohnerinnen und Bewohner nur aufgrund einer Einwilligungserklärung zulässig ist. Zudem ist bei der Erhebung der Biografiedaten der Grundsatz der Datenerhebung beim Betroffenen zu beachten, wonach personenbezogene Daten beim Betroffenen zu erheben sind und eine Datenerhebung bei Dritten nur in Ausnahmefällen zulässig ist. Diese Anforderungen sind von einigen Pflegeheimen umgehend umgesetzt worden. Zum Teil wurde in diesem Zusammenhang auch von einigen Pflegeheimen signalisiert, dass die Datensammlungen wegen der teilweise erheblichen Eingriffe in das Persönlichkeitsrecht der Betroffenen kritisch gesehen würden. Der Träger eines Pflegeheims weigerte sich mit der Begründung eines erhöhten Verwaltungsaufwands und unter Hinweis darauf, dass viele andere Pflegeheime die Biografiedaten auch ohne Einwilligung erhöben, unsere Anforderungen umzusetzen. Um in allen Pflegeheimen ein datenschutzgerechtes Vorgehen durchzusetzen, traten wir an die Heimaufsicht heran und baten um Unterstützung in dieser Angelegenheit. Daraufhin wurde von der Heimaufsicht ein Arbeitskreis unter Beteiligung von Pflegeheimen, Pflegewissenschaftlern, Angehörigen und der Landesbeauftragten für Datenschutz und Informationsfreiheit eingerichtet, der sich mit dem Thema Biografiearbeit beschäftigte. Im Arbeitskreis herrschte Einigkeit darüber, dass Biografiedaten nur auf freiwilliger Basis erhoben werden dürfen. Es stellte sich jedoch heraus, dass es keine einheitliche Auffassung dazu gibt, was unter Biografiearbeit zu verstehen ist. Ebenso gibt es in den Pflegeheimen kein einheitliches Verfahren für die Erhebung und Verarbeitung von Biografiedaten. Der Arbeitskreis hat sich daher entschlossen, einen Leitfaden zum datenschutzgerechten Umgang bei der Biografiearbeit in Pflegeheimen zu erarbeiten, dieser befand sich bei Redaktionsschluss noch in der Abstimmung.

## 13.8 Handel, Handwerk und Dienstleistungen

### 13.8.1 Kopien des Führerscheins und des Personalausweises durch ein Carsharing-Unternehmen

Auf unsere Anfrage hin hat ein Carsharing-Unternehmen eingeräumt, bei Neukundinnen und Neukunden werde der Führerschein oder Personalausweis kopiert, es sei denn, dem werde durch die Kundinnen und Kunden widersprochen. Als Grund wurde angegeben, bei Informationsveranstaltungen sei meistens keine Zeit, die genaue Prüfung der Dokumente und die Gegenprüfung mit den Angaben zum gerade abgeschlossenen Vertrag vorzunehmen. Die Kopien würden später zu den Verträgen abgelegt.

Wir haben dem Unternehmen erklärt, dass das Verfahren nicht den Anforderungen des Bundesdatenschutzgesetzes (BDSG) entspricht. Danach dürfen personenbezogene Daten nur erhoben und gespeichert werden, soweit sie für den Vertragszweck erforderlich sind. Da sowohl der Führerschein als auch der Personalausweis eine Vielzahl von Daten enthalten, die für die Eingehung eines Carsharing-Vertrages nicht erforderlich sind, ist die Anfertigung von Kopien davon nicht zulässig. Soweit das rechtmäßige Verhalten mit einem nach Angaben des Unternehmens dar-

gelegten erheblichen Aufwand verbunden wäre, bestünde die Möglichkeit, potenzielle Vertragspartnerinnen und Vertragspartner um eine den Anforderungen des BDSG entsprechende Einwilligung zu bitten, die Dokumente zum Abgleich mit den Vertragsdaten zu kopieren und sie danach unverzüglich zu vernichten. Da die gesetzlichen Anforderungen an die Einwilligung in den zurückliegenden Fällen nicht vorgelegen haben, haben wir das Unternehmen aufgefordert, die bisherigen Kopien zu vernichten. Das Unternehmen hat daraufhin mitgeteilt, auf die Anfertigung von Kopien zukünftig zu verzichten und später hinzugefügt, die bisherigen Kopien nach und nach vernichtet zu haben.

### 13.8.2 Anfertigung von Personalausweiskopien bei Besuchern einer Freizeiteinrichtung

Bei einigen Unternehmen besteht die Geschäftsübung, Kundinnen und Kunden am Tage deren Geburtstags besondere Vergünstigungen bei Einkäufen, Dienstleistungen und so weiter anzubieten. Ein Unternehmen der Freizeitbranche gewährte seinen Kundinnen und Kunden, die am Besuchstag Geburtstag hatten, gegen entsprechenden Nachweis kostenlosen Eintritt zu seinen Einrichtungen. Das Kassenpersonal war jedoch gehalten, als Nachweis dafür, dass der kostenlose Eintritt tatsächlich einem Geburtstagskind gewährt wurde, eine Kopie der Vorderseite des Personalausweises oder eines anderen amtlichen Ausweises mit dem eingetragenen Geburtsdatum anzufertigen. Die Ausweiskopie wurde sodann zum Zweck der späteren Richtigkeitskontrolle der Abrechnungen des Kassenpersonals zu den Abrechnungsunterlagen genommen und erst nach Abschluss der Abrechnungskontrolle vernichtet.

Diese Praxis stieß berechtigterweise auf Kritik von Besucherinnen und Besuchern. Auf eine entsprechende Beschwerde hin wandten wir uns daher an das Unternehmen und wiesen darauf hin, dass diese Praxis mit den Regelungen des Bundesdatenschutzgesetzes (BDSG) nicht im Einklang stehe. Zwar dürfen grundsätzlich diejenigen Daten erhoben und verwendet werden, die für die Begründung, Durchführung oder Beendigung eines Vertrages erforderlich sind. Vorliegend kann jedoch der Vertrag regelmäßig anonym und beidseitig sofort abgewickelt werden, weil der Eintritt zur beziehungsweise die Nutzung der Freizeiteinrichtung nur gegen sofortige Zahlung gewährt wird und die Identität der Besucherin oder des Besuchers in diesem Zusammenhang völlig unerheblich ist. Für den Fall, dass die Besucherin oder der Besucher die Geburtstagsvergünstigung in Anspruch nehmen will, kann selbstverständlich ein entsprechender Nachweis des Geburtstags verlangt werden. Dieser Nachweis ist jedoch seitens der Kundin oder des Kunden bereits erbracht, wenn dem Kassenpersonal ein Ausweisdokument mit dem entsprechenden Geburtstagsdatum zur Kenntnisnahme vorgelegt ist. Einer Ausweiskopie bedarf es hierfür nicht. Die in der Kopieanfertigung liegende Erhebung und Speicherung des Namens der Besucherin oder des Besuchers und erst recht der übrigen auf der Personalausweisvorderseite befindlichen personenbezogenen Daten, wie Lichtbild, Geburtsjahr, Geburtsort, Nationalität, Ausweisgültigkeit, Ausweisnummer, war daher für die Vertragszwecke offensichtlich nicht erforderlich und damit nach § 28 Absatz 1 Satz 1 Ziffer 1 BDSG unzulässig. Das Unternehmen reagierte auf unseren Hinweis erfreulicherweise umgehend und stellte die Praxis der Anfertigung von Ausweiskopien ein.

### 13.8.3 Durchsetzung datenschutzrechtlicher Ansprüche Betroffener gegenüber sogenannten Kaffeefahrt-Unternehmen

Wie schon in früheren Jahren erhielten wir auch im aktuellen Berichtszeitraum etliche Beschwerden von Bürgerinnen und Bürgern, die als Gewinnbenachrichtigung deklarierte Werbepost von Kaffeefahrt-Unternehmen erhalten und daraufhin versucht hatten, entsprechend ihres datenschutzrechtlichen Auskunftsanspruchs nach § 34 Bundesdatenschutzgesetz (BDSG) von dem Unternehmen Auskunft darüber zu erlangen, welche Daten dieses über sie gespeichert, und gegebenenfalls, an wen es diese weitergegeben hat. Oftmals widersprachen die Betroffenen zugleich auch der weiteren Verarbeitung beziehungsweise Nutzung ihrer Daten für Werbezwecke. Die Ausübung dieses Werbewiderspruchsrechts nach § 28 Absatz 4 Satz 1 BDSG führt zur Unzulässigkeit der weiteren Datenverwendung für Werbezwecke. Setzt sich ein Unternehmen hierüber hinweg, indem es die Daten weiter für Werbezwecke verwendet, so stellt dies seit der Novellierung des Bundesdatenschutzgesetzes in 2009 in der Regel eine Ordnungswidrigkeit dar, die mit einer Geldbuße bis zu

300.000 Euro geahndet werden kann. Nachdem keinerlei Reaktion der Unternehmen erfolgte, wandten sich die Betroffenen an uns. Bei der Durchsetzung der Rechte der Betroffenen gegenüber diesen Unternehmen sind wir jedoch regelmäßig mit dem Problem konfrontiert, dass es sich bei den fraglichen Unternehmen zumeist um reine Postfachfirmen handelt und daher verantwortliche Personen mit den uns zur Verfügung stehenden Mitteln und Ressourcen nicht zu ermitteln sind. Die Möglichkeit der rechtlichen Durchsetzung der datenschutzrechtlichen Ansprüche Betroffener stößt in diesen Fällen an tatsächliche Grenzen. Uns bleibt oftmals nur die Möglichkeit, auf eine Stilllegung des Postfachs des jeweiligen Unternehmens hinzuwirken. Es muss damit weiterhin bei der generellen Empfehlung bleiben, sich auf diese Kaffeefahrt-Unternehmen beziehungsweise ihre Werbepost nicht einzulassen.

### 13.8.4 Prüfung von Onlineshops

Im Jahr 2008 haben wir die Verarbeitung von Nutzerdaten in Onlineshops geprüft. Der Vorgang konnte allerdings erst in diesem Jahr abgeschlossen werden, da bei einigen Shops die Umsetzung unserer datenschutzrechtlichen Vorgaben sehr schleppend verlief. In zwei Fällen mussten wir die Verhängung von Zwangsgeldern androhen. Da wir nur stichprobenartig prüfen konnten, möchten wir die Bürgerinnen und Bürger im Hinblick auf die Übermittlung personenbezogener Daten in Onlineshops auf diesem Weg sensibilisieren.

**Blick ins Impressum**

Zunächst empfiehlt sich ein Blick in das Impressum. Das Impressum soll Verbraucherinnen und Verbraucher mit Hilfe der dort enthaltenen Angaben in die Lage versetzen, die Onlineanbieter auf ihre Seriosität zu überprüfen, zum Beispiel durch Anruf bei den zuständigen Aufsichtsstellen, bevor sie deren Dienste in Anspruch nehmen. Zudem haben die Nutzerinnen und Nutzer auf diese Weise Kontaktdaten für den Beschwerdefall und wissen, wo sich der Sitz des Unternehmens befindet. Das Impressum sollte auf jeden Fall Informationen wie den Namen, die Anschrift und die E-Mail-Adresse des Anbieters enthalten. Hat ein Onlineshop kein Impressum, ist Vorsicht geboten.

**Durchsicht der Datenschutzerklärung**

Weiterhin sollte die Datenschutzerklärung gelesen werden. Dieser kann entnommen werden, ob die Daten nur zur Vertragsabwicklung verarbeitet werden und im Unternehmen bleiben oder ob sie auch an Dritte weitergegeben werden. Es kann zum Beispiel sein, dass das Unternehmen eine Bonitätsanfrage bei einer Auskunftei stellt. Die Nutzerinnen und Nutzer sollten sich dann genau überlegen, ob sie mit der geplanten Verwendung der Daten auch wirklich einverstanden sind oder doch lieber von dem Kauf Abstand nehmen.

**Eingabe personenbezogener Daten**

Ab dem Moment, wo die Nutzerinnen und Nutzer personenbezogene Daten preisgeben müssen, sollte eine gesicherte Verbindung, zum Beispiel SSL-Verschlüsselung, durch den Onlineshop angeboten werden. Ansonsten kann jedermann die Datenübermittlung mitlesen. Ob gesicherte Verbindungen verwendet werden, ist an dem angezeigten Protokoll „https://“ zu Beginn der Adresszeile im Browser oder meistens an einem kleinen Vorhängeschloss mit geschlossenem Bügel zu erkennen.

**Zahlungsmodalitäten**

Es empfiehlt sich – wenn der Onlineshop dies anbietet – auf Rechnung zu bestellen. Dann müssen keine Bankverbindungsdaten übermittelt werden. Die Weitergabe von Kontodaten birgt stets Missbrauchsgefahren. Sollte die Eingabe von Bankverbindungsdaten unerlässlich sein, ist umso mehr auf eine gesicherte Verbindung zu achten.

### 13.8.5 Aufzeichnung von Telefongesprächen zur Störungsbeseitigung durch einen Energieversorger

Auf der Homepage eines Energieversorgers fanden wir Hinweise über die Aufzeichnung von Telefongesprächen. Wir fragten dort an, zu welchen Zwecken diese Gesprächsaufzeichnungen erforderlich seien, wie lange die Aufzeichnungen gespeichert würden und welche Rechtsvorschrift dies erlaube. Der Energieversorger erklärte, es würden alle Telefongespräche aufgezeichnet, um in Gefahrenfällen, zum

Beispiel bei Gasausbruch, keine Zeit zu verlieren. Ein Abhören der Aufzeichnungen erfolge nur im Beisein mindestens einer Führungskraft und des Betriebsrats. Die Aufzeichnungen würden rund drei Monate aufbewahrt. Die Möglichkeit der Dokumentation in Form von Gesprächsaufzeichnungen sei in einem Arbeitsblatt genannt, in dem Grundsätze und Organisation des Bereitschaftsdienstes für Gas- und Wasserversorgungsunternehmen festgelegt seien. Das Arbeitsblatt gelte für alle Versorgungseinrichtungen und Kundenanlagen, die in der öffentlichen Versorgung betrieben werden.

Wir wiesen den Energieversorger auf die Rechtslage hin. Danach verletzt eine Gesprächsaufzeichnung das Recht am gesprochenen Wort beziehungsweise an der Vertraulichkeit des gesprochenen Wortes, soweit dies nicht gesetzlich erlaubt ist oder beide Gesprächspartner darin eingewilligt haben. Soweit die Aufzeichnung zur unverzüglichen Klärung und Beseitigung der Störung erforderlich ist, reicht eine Aufbewahrung über maximal 24 Stunden aus, wie dies auch bei der Feuerwehr und der Polizei nach speziellen Rechtsvorschriften vorgesehen ist. Außerdem ist zu diesem Zweck nicht die Anwesenheit einer Führungskraft und auch nicht des Betriebsrats erforderlich. Es reicht vollkommen aus, wenn die für die Beseitigung der Störung zuständigen Beschäftigten des Energieversorgers Gespräche in den akuten Fällen abhören, wenn dies zur Feststellung des Ortes der Störung erforderlich ist.

Der Energieversorger hat daraufhin zugesichert, die Gesprächsaufzeichnungen nach 24 Stunden zu löschen und dies mit im Einzelnen nachvollziehbaren technischen und organisatorischen Maßnahmen zu gewährleisten. Außerdem würden künftig nur noch zuständige Beschäftigte im erforderlichen Einzelfall ein Gespräch nachträglich abhören.

### 13.8.6 Reichweitenmessung bei Internetangeboten

Vielfach analysieren Website-Betreiber zu Zwecken der Werbung und Marktforschung sowie zur bedarfsgerechten Gestaltung ihres Internetangebotes das Surfverhalten von Nutzerinnen und Nutzern. Zur Erstellung solcher Nutzerprofile verwenden sie oftmals Software beziehungsweise Dienste, die von Dritten angeboten werden.

Da Websites häufig von externen Dienstleistern gestaltet und verwaltet werden, ist den Website-Betreibern nicht immer der Einsatz solcher Analysetechniken überhaupt bewusst oder bekannt. Dennoch sind sie als Auftraggeber für die Erstellung von Nutzungsprofilen verantwortlich. Dies ergibt sich aus den Regelungen des Bundesdatenschutzgesetzes (BDSG) zur Auftragsdatenverarbeitung.

Bei der Erstellung von Nutzungsprofilen sind die Regelungen des Telemediengesetzes (TMG) zu beachten. Hiernach dürfen Nutzungsprofile nur bei Verwendung von Pseudonymen erstellt werden. Die IP-Adresse ist kein Pseudonym im Sinne des Telemediengesetzes, sondern ein personenbezogenes Datum.

Genaue Anforderungen an den Einsatz von Analyseverfahren haben die obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich, der sogenannte Düsseldorfer Kreis, in einem Beschluss auf der Sitzung im November 2009 festgelegt (vergleiche Ziffer 17.8 dieses Berichts).

## 13.9 Kreditwirtschaft

### 13.9.1 Unzureichende Datenschutzvorkehrungen bei SB-Zahlungsverkehrsterminals der Sparkassen

Aufgrund zweier Beschwerden überprüften wir im Berichtszeitraum unter anderem auch die Datenschutzvorkehrungen bei den erst seit Kurzem installierten SB-Zahlungsverkehrsterminals neuerer Generation stichprobenweise in Filialen der Sparkassen Bremen und Bremerhaven.

Bei unserer Überprüfung stellten wir fest, dass die Displays dieser SB-Terminals neuerer Generation erhöht über dem Gerät angebracht, vertikal ausgerichtet und seitlich abgeflacht sind. Die Schriftbildanzeige der Bildschirme war im Vergleich zu den Einstellungen bei den bisherigen SB-Terminals deutlich vergrößert, um – wie uns mitgeteilt wurde – eine bessere Lesbarkeit für die Nutzerinnen und Nutzer zu erreichen. Sichtschutzwände oder ähnliche organisatorische Sicherheitsvor-

kehrungen, wie etwa eine Ausrichtung der Displays zur Wand, existierten bei den SB-Terminals in den überprüften Filialräumlichkeiten nicht. Verschärft wurde die Situation zum Teil noch durch besondere räumliche Gegebenheiten, welche die Einhaltung eines Diskretionsabstandes zwischen SB-Terminalnutzenden und gegebenenfalls weiteren wartenden Kundinnen und Kunden erschwerten. Zusammenfassend musste festgestellt werden, dass wirksame Vorkehrungen zum Ausschluss eines Mitlesens der Eingaben beziehungsweise Anzeigen durch Dritte bei den SB-Terminals in den überprüften Filialräumlichkeiten nicht existierten.

Nach dem Bundesdatenschutzgesetz beziehungsweise auch dem Landesdatenschutzgesetz ist jede verantwortliche Stelle verpflichtet, datenschutzrechtlichen Anforderungen genügende technische und organisatorische Schutzvorkehrungen bei einer automatisierten Datenverarbeitung zu treffen. Hierzu gehört insbesondere auch eine – wirksame – Sicherung gegen unbefugtes Mitlesen beim Umgang mit personenbezogenen Daten. Die vorgefundene Situation bei den SB-Terminals genügte diesen datenschutzrechtlichen Anforderungen offenkundig nicht. Die betroffenen Kreditinstitute wurden darauf hingewiesen, dass die automatisierte Datenverarbeitung an den SB-Terminals unter dem Gesichtspunkt der sogenannten Zugriffskontrolle nicht im Einklang mit geltendem Datenschutzrecht steht. Sie wurden zur Beseitigung des insoweit unzulässigen Zustands aufgefordert.

Die betroffenen Kreditinstitute sicherten zu, im Wege technischer Veränderungen des Schriftbildes für Abhilfe zu sorgen. Diese Veränderungen werden nicht dezentral durch die Kreditinstitute, sondern durch einen zentralen IT-Dienstleister umgesetzt. Dies ist die Begründung der Kreditinstitute dafür, dass der Abschluss dieser Maßnahme noch aussteht. In einem ersten Schritt wurden einstweilige Schutzmaßnahmen, etwa das Anbringen neuer Diskretionsmarken, ergriffen. Es bleibt nunmehr abzuwarten, ob die technische Veränderung des Schriftbildes ausreichenden Schutz schafft. Wir werden dies genau beobachten und gegebenenfalls auf weitere Schutzmaßnahmen dringen, bis Mitlesemöglichkeiten Dritter an den SB-Terminals so weit wie möglich ausgeschlossen sind.

### 13.9.2 Einzug der EC-Karte am Bankautomaten nach Todesfall

Einige Tage nach dem Tod einer nahe stehenden Person wollte ein Angehöriger, dem zu Lebzeiten eine Vollmacht für das Konto der verstorbenen Person eingeräumt worden war, noch die Kontoauszüge bei dem kontoführenden Kreditinstitut am Automaten ausdrucken. Eine Sterbeurkunde oder gar ein Erbschein waren dem kontoführenden Kreditinstitut zu diesem Zeitpunkt noch nicht vorgelegt worden. Gleichwohl wurde die EC-Karte aufgrund einer entsprechenden Anweisung des Kreditinstituts am Automaten eingezogen. Der Angehörige wunderte sich hierüber und wandte sich mit der Frage an uns, ob Kreditinstitute von amtlicher Seite über Todesfälle informiert würden.

Kreditinstitute erhalten jedoch keine Mitteilung von Amts wegen über einen Todesfall. Die einschlägigen Gesetze, namentlich das Personenstandsgesetz und die ausführende Personenstandsverordnung, sehen keine offizielle Benachrichtigung privater Stellen vor. Eine derartige Benachrichtigung würde im Übrigen in der Praxis auch voraussetzen, dass die entsprechenden amtlichen Stellen (in erster Linie das Standesamt, sodann Meldeamt, Nachlassgericht und so weiter) durchgängig über sämtliche Bankverbindungen der oder des Verstorbenen Bescheid wüssten, um die Nachricht vom Tod weitergeben zu können. Kreditinstitute werten jedoch unter Umständen die Todesanzeigen örtlicher Tageszeitungen aus. Auch vorliegend war in einer Tageszeitung einige Tage nach dem Tod eine Todesanzeige erschienen. Allerdings kann die Richtigkeit einer Todesanzeige oder sonstiger Mitteilungen über einen Todesfall bei Bedarf über eine Registerauskunft überprüft werden. Sowohl das Personenstandsgesetz als auch das Meldegesetz kennen ein Recht auf Auskunft aus dem Personenstandsregister, hier konkret Sterberegister beziehungsweise Melderegister, sofern die Interessentin oder der Interessent ein rechtliches Interesse glaubhaft macht. Kreditinstitute besitzen ein derartiges Interesse an der Kenntnis eines Todesfalles, da sie zivilrechtlich grundsätzlich nur durch Leistungen an den oder die tatsächlichen Erben von ihren Verpflichtungen frei werden, im Übrigen gemäß § 33 Erbschaftssteuergesetz grundsätzlich dazu verpflichtet sind, die bei ihnen befindlichen Vermögensgegenstände der Erblasserin oder des Erblassers dem zuständigen Finanzamt gegenüber – regelmäßig binnen eines Monats – anzuzeigen. In den meisten Fällen werden die Kreditinstitute jedoch erst durch Familienangehörige über einen Todesfall in der Familie unterrichtet.

## 13.10 Vereine

### 13.10.1 Datenschutz in Kleingartenvereinen

Im Jahr 2009 haben wir verschiedene Kleingartenvereine in Bremen besucht und deren Mitgliederdatenverwaltung geprüft. Der Datenschutz hat in diesem Feld eine große Bedeutung und wurde überwiegend beachtet.

Im Rahmen der Prüfung wurden folgende Aspekte datenschutzrechtlich gewürdigt:

— Aufnahmebogen für die neuen Pächterinnen oder Pächter beziehungsweise neuen Kleingartenmitglieder,

— Mitteilung des Berufs der Pächterin oder des Pächters beziehungsweise Kleingartenmitglieds vom Vorstandsmitglied an die Wegewartin oder den Wegewart zur Einteilung des Gemeinschaftsdienstes,

— Veröffentlichung von personenbezogenen Daten im Internet, wie zum Beispiel Fotografien des Sommerfestes oder private Telefonnummern von Vorstandsmitgliedern,

— Zusendung aktualisierter Mitgliederlisten per E-Mail zwischen den Vorstandsmitgliedern,

— Übermittlung von Mitgliederdaten durch den Vorstand an den Verlag zum Versand der Mitgliederzeitschrift,

— Datenschutzerklärung und Satzungsänderung,

— Verpflichtung des Vorstands auf das Datengeheimnis,

— technische und organisatorische Maßnahmen sowie

— Vernichtung von Unterlagen.

Die Mitgliederaktenverwaltung ist in den Kleingartenvereinen sehr unterschiedlich organisiert, in manchen Kleingartenvereinen gibt es nur die Papieraktenführung.

Unter den Kleingartenvereinen herrschte erhebliche Unsicherheit hinsichtlich der rechtlichen Anforderungen nach dem Bundesdatenschutzgesetz (BDSG). Das derzeitige Verfahren zur Versendung der Mitgliederzeitschrift durch den Landesverband der Gartenfreunde Bremen e. V. – im folgenden Landesverband genannt – stellt sich so dar, dass der Landesverband einen Vertrag mit dem Verlag über die Herstellung und Versendung der Mitgliederzeitschrift hat. Im Rahmen dieses Vertrages wird das jeweils pro Kleingartenverein zuständige Vorstandsmitglied zwecks Aktualisierung von Namen und Privatadressen vom Verlag angeschrieben, damit eine Versendung durch den Landesverband über den Verlag erfolgen kann. Der Landesverband selbst besitzt keine Liste über alle Mitgliedsnamen und Privatadressen. Der Verlag verarbeitet die Daten im Auftrag des Landesverbands. Hier sind die Anforderungen, die § 11 BDSG an den Auftraggeber, also an den Landesverband stellt, einzuhalten. Die Versendung der Mitgliederzeitschrift dient sowohl dem Vereinszweck, § 2 der Vereinssatzung, als auch den Interessen der Mitglieder im Rahmen ihrer Mitgliedschaft und erlaubt damit gemäß § 28 Absatz 1 Satz 1 Nummer 2 BDSG eine Datenübermittlung der Mitgliederdaten, jedoch nur Name und Privatanschrift, an den Verlag für den Versand.

Hinsichtlich der Aufnahme von Datenschutzbestimmungen im Rahmen einer Satzungsänderung ist zu beachten, dass eine Einwilligung erforderlich ist, soweit die Datenverarbeitung nicht von § 28 BDSG als gesetzliche Grundlage erlaubt ist. Grundsätzlich sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit ein Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder das betroffene Mitglied eingewilligt hat. Eine Satzungsbestimmung einer juristischen Person des Privatrechts wie einem Kleingartenverein ist keine Rechtsvorschrift in diesem Sinne. Somit kann eine Änderung der Vereinssatzung die jeweiligen Einwilligungen der Mitglieder nicht ersetzen. Wir empfahlen aus diesem Grund, in die Vereinssatzung eine Datenschutzbestimmung hinsichtlich der Verwaltung der Mitgliederdaten mit aufzunehmen. Diese Datenschutzbestimmung soll die Zwecke, für die die Daten verarbeitet oder genutzt werden, gemäß § 28 Absatz 1 Satz 2 BDSG konkret festlegen. Weiter können Regelungen aufgenommen werden, die die ordnungsgemäße Datenverarbeitung betreffen, zum Beispiel welche Daten zu welchem Zweck in welcher Form von wem verarbeitet

oder genutzt werden dürfen. Auch sollten die technischen und organisatorischen Maßnahmen betreffend die Datensicherheit gemäß § 9 BDSG bestimmt werden, zum Beispiel die Verpflichtung zur Erstellung einer Liste der Schlüsselbesitzerinnen und Schlüsselbesitzer für Tresor oder Stahlschrank oder Vereinsheim, Regelungen zur Vernichtung von Unterlagen mit personenbezogenen Daten sowohl bezüglich der Art und Weise der Vernichtung als auch bezüglich der Frist, ab wann eine Vernichtung von Dokumenten stattzufinden hat.

Datenschutzrechtlich unzulässig war eine Kleingartenmitgliederakte, die noch einen Pachtvertrag aus dem Jahre 1938 enthielt und damit gegen die Löschungsverpflichtung für nicht mehr erforderliche Daten nach BDSG verstieß. Wir haben den betroffenen Kleingartenverein darauf hingewiesen.

Zur Verbesserung des technischen und organisatorischen Datenschutzes haben wir einige Anforderungen aufgestellt und Vorschläge unterbreitet, so beispielweise zur Einrichtung eines Zugangsschutzes zu DV-Systemen, zu Schutzmaßnahmen gegen Angriffe aus dem Internet, zur Durchführung von Administrationstätigkeiten durch Dritte, zur Verschlüsselung personenbezogener Daten auf der Festplatte sowie zur datenschutzgerechten Vernichtung von Unterlagen. Darüber hinaus haben wir dem Landesverband der Gartenfreunde Bremen ein Merkblatt für die technischen und organisatorischen Maßnahmen zur Verfügung gestellt.

Aufgrund der kooperativen Zusammenarbeit, sowohl mit den Kleingartenvereinen als auch mit dem Landesverband, gehen wir von einer Beseitigung der sehr geringen datenschutzrechtlichen Mängel aus und befürworten weiterhin die Änderung der jeweiligen Kleingartensatzung unter Aufnahme von Datenschutzbestimmungen.

### 13.11 Ordnungswidrigkeitsverfahren nach dem Bundesdatenschutzgesetz

Im Jahr 2009 wurden von uns drei Ordnungswidrigkeitsverfahren wegen Verstoßes gegen das Bundesdatenschutzgesetz (BDSG) betrieben, in zwei Verfahren wurden Bußgeldbescheide erlassen. Nachdem wir festgestellt hatten, dass die Videoüberwachung, die ein Anwohner in einer Eigentumswohnanlage durchführte, unzulässig ist, hatten wir diesen aufgefordert, die von ihm verwendeten Videokameras unverzüglich zu entfernen und uns darüber zu informieren. Der Anwohner hatte uns daraufhin mitgeteilt, dass die von ihm verwendeten Videokameras abgebaut und der rechtswidrige Zustand beseitigt worden sei. Wie unsere Überprüfung dann später ergab, hatte der Anwohner keine korrekte Auskunft erteilt, der Rechtsverstoß bestand auch weiterhin. Wegen des Verstoßes gegen § 43 Absatz 1 Nummer 10 BDSG, wonach unter anderem ordnungswidrig handelt, wer vorsätzlich oder fahrlässig eine Auskunft nicht richtig erteilt, wurde gegen den Anwohner von uns ein Bußgeldbescheid erlassen und ein Bußgeld in Höhe von 800 Euro festgesetzt. Der Betroffene hat gegen den Bußgeldbescheid Einspruch eingelegt. Da wir den Bescheid aufrechterhalten, wird der Vorgang zur weiteren Bearbeitung voraussichtlich an die Staatsanwaltschaft abgegeben werden.

In dem zweiten Fall erließen wir einen Bußgeldbescheid gegen den Inhaber einer Auskunftei wegen eines Verstoßes gegen die Meldepflicht nach § 4 d BDSG. Nach § 43 Absatz 1 Nummer 1 BDSG handelt unter anderem ordnungswidrig, wer eine Meldung zu dem von uns nach § 38 Absatz 2 BDSG geführten Register der nach § 4 d BDSG meldepflichtigen automatisierten Verarbeitungen nicht richtig oder nicht vollständig macht. Trotz wiederholter Aufforderung hatte der Meldepflichtige seine Meldung nicht, wie es erforderlich gewesen wäre, ergänzt beziehungsweise verändert. Mit dem Bußgeldbescheid setzten wir in diesem Fall ein Bußgeld in Höhe von 300.000 Euro fest. Der Bußgeldbescheid ist rechtskräftig geworden, die Zahlung der Geldbuße ist inzwischen erfolgt.

Noch kein Bußgeldbescheid ist im dritten Ordnungswidrigkeitsverfahren erlassen worden, das gegen ein Zeitungsunternehmen begonnen wurde. Das Verfahren wegen unbefugter Datenerhebung und -speicherung sowie unterlassener Benachrichtigung der von der Erhebung und Speicherung Betroffenen befindet sich zurzeit noch in der Phase der Anhörung (vergleiche Ziffer 13.5.5 dieses Berichts).

## 14. Datenschutz auf europäischer und internationaler Ebene

### 14.1 Die Volkszählung im Jahr 2011

Aufgrund der Verordnung des Europäischen Parlaments und des Rates vom 9. Juli 2008 über Volks- und Wohnungszählungen wird in allen Mitgliedstaaten der Euro-

päischen Union erstmals im Jahr 2011 eine europaweite Erhebung von Bevölkerungsdaten sowie Daten über die Wohnungssituation stattfinden. Auch Deutschland wird sich an dieser Volks- und Wohnungszählung beteiligen. Das Statistische Landesamt informiert bereits seit einiger Zeit auf seiner Homepage und durch gelegentliche Zeitungsberichte über den anstehenden Zensus 2011.

Die letzten Volkszählungen fanden in der Bundesrepublik Deutschland im Jahr 1987, in der ehemaligen Deutschen Demokratischen Republik im Jahr 1981 statt. Seitdem wurden die dabei erhobenen Bevölkerungszahlen lediglich amtlich fortgeschrieben. Der Zensus 2011 soll nunmehr aktuelle und verlässliche Datengrundlagen für gesellschaftliche, politische und wirtschaftliche Planungen liefern.

Der Volkszählung im Jahr 1987 waren tief greifende öffentliche Diskussionen, begründet in der Sorge breiter Bevölkerungskreise vor einer umfassenden staatlichen Durchleuchtung, vorangegangen. In seinem Volkszählungsurteil vom 15. Dezember 1983 formulierte das Bundesverfassungsgericht, ausgehend von dem in diesem Urteil aus der Taufe gehobenen Grundrecht auf informationelle Selbstbestimmung, grundlegende Anforderungen an die Durchführung von Erhebungen personenbezogener Daten für amtliche statistische Zwecke. Die Vorgaben des Bundesverfassungsgerichts prägten im Anschluss die Gesetzgebung. Auch die Durchführung des Zensus 2011 muss sich an diesen Vorgaben des Bundesverfassungsgerichts ausrichten.

Die gesetzlichen Grundlagen für die Zensuserhebungen finden sich maßgeblich im Zensusvorbereitungsgesetz 2011, auf dessen Grundlage seit Frühjahr 2008 beim Statistischen Bundesamt ein Anschriften- und Gebäuderegister aufgebaut und kontinuierlich aktualisiert wird, sowie im Zensusgesetz 2011.

Im Unterschied zur letztmaligen Volkszählung in der Bundesrepublik Deutschland wird der Zensus 2011 im Wesentlichen im Wege der Erhebung, Zusammenführung und Auswertung von Melderegisterdaten der Meldebehörden, Daten der Bundesagentur für Arbeit und Daten anderer Verwaltungsregister zum Berichtszeitpunkt 9. Mai 2011 bei den Statistischen Ämtern des Bundes und der Länder durchgeführt. Persönliche Befragungen der Einwohnerinnen und Einwohner werden auf ein minimales Maß begrenzt. Lediglich Verwalterinnen und Verwalter, Eigentümerinnen und Eigentümer sowie sonstige Verfügungsberechtigte von Gebäuden und Wohnungen werden ergänzend zum Zwecke der Erhebung von Daten zur Wohnsituation – mangels insoweit verfügbarer staatlicher Registerdaten – auf postalischem Weg voraussichtlich gegen Ende des Jahres 2010 direkt befragt. Hinzu kommt zur Qualitätsabsicherung und Erlangung weiterer, ergänzender Zensusmerkmale eine direkte Haushaltebefragung auf Stichprobenbasis bei bis zu maximal 10 Prozent der Bevölkerung. Eine direkte Erhebung erfolgt sodann noch für Bewohnerinnen und Bewohner von sogenannten Sonderbereichen, wie Gemeinschafts-, Anstalts- und Notunterkünfte, Wohnheime und ähnliche Unterkünfte.

Der weitgehende Verzicht auf direkte beziehungsweise persönliche Befragungen der Einwohnerinnen und Einwohnern reduziert zwar die unmittelbare Belastung, ist jedoch datenschutzrechtlich nicht weniger problematisch oder weniger eingriffsintensiv. Den Einwohnerinnen und Einwohnern wird nämlich nicht mehr unmittelbar ersichtlich, welche personenbezogenen Daten über sie im Einzelnen erhoben und für Statistikzwecke verwendet werden. Schon im Volkszählungsurteil hatte das Bundesverfassungsgericht auch Bedenken gegen eine Volkszählung geäußert, die allein im Wege einer Übernahme und Nutzung sämtlicher Daten aus bereits vorhandenen unterschiedlichen Registern zu statistischen Zwecken durchgeführt wird.

Datenschutzrechtliche Bedenken bestehen wegen der Gefahr sozialer Abstempelung auch gegen die personenbezogene Datenerhebung in Sonderbereichen und sogar sensiblen Sonderbereichen, zum Beispiel Obdachlosenunterkünfte, Justizvollzugsanstalten. Auch mit dieser Frage hatte sich das Bundesverfassungsgericht befasst und für die Volkszählung 1987 ausdrücklich empfohlen, auf eine personenbezogene Erhebung zu verzichten und stattdessen eine anonyme Erhebung bei der Leiterin oder dem Leiter der Einrichtung durchzuführen. Der Gesetzgeber hielt jedoch unter Hinweis auf die aus einer anonymen Erhebung möglicherweise resultierenden Ungenauigkeiten in der Bevölkerungserfassung trotz aller Kritik der Datenschutzbeauftragten an der personenbezogenen Erhebung fest. Gewisse Ungenauigkeiten sind jedoch im Rahmen eines solch umfassenden, noch nie da gewesenen Datenerhebungsprogramms ohnehin nicht auszuschließen, und es ist stark zu bezweifeln, dass gerade die anonyme Erhebung in diesen Bereichen zu gravie-

renden statistischen Fehlern geführt hätte. Es muss nun auf jeden Fall im Rahmen der Durchführung sichergestellt werden, dass der Personenbezug durch frühestmögliche Löschung umgehend aufgelöst wird.

Datenschutzrechtlich zu bemängeln ist des Weiteren, die im Zensusvorbereitungsgesetz vorgesehene Rückübermittlung der Anschriftenbereiche, zu denen Anhaltspunkte auf unvollständige oder fehlerhafte Daten vorliegen, von den statistischen Landesämtern an die Meldebehörden. Sie steht im Widerspruch zur notwendigen strikten Abschottung des Statistikbereichs gegenüber dem Bereich des Verwaltungsvollzugs, wie sie seitens des Bundesverfassungsgerichts im Volkszählungsurteil postuliert wurde. Zitat: „Für den Schutz des Rechts auf informationelle Selbstbestimmung ist – und zwar auch schon für das Erhebungsverfahren – die strikte Geheimhaltung der zu statistischen Zwecken erhobenen Einzelangaben unverzichtbar, solange ein Personenbezug noch besteht oder herstellbar ist . . .“ Trotz entsprechend geäußerter Kritik hielt der Gesetzgeber an der fraglichen Regelung fest.

Wenngleich im Gesetzgebungsverfahren zum Zensus 2011 auf Anregung der Datenschutzbeauftragten einige datenschutzrechtliche Kritikpunkte beseitigt wurden, so zeigen bereits die eben genannten Beispiele, dass der Zensus 2011 in einigen Punkten durchaus weiterhin zu datenschutzrechtlichen Bedenken Anlass gibt. Die weitere Durchführung der Volkszählung wird daher seitens der Datenschutzbeauftragten in Bund und Ländern aufmerksam zu beobachten sein.

### 14.2 Stockholmer Programm der Europäischen Union

Unter der schwedischen EU-Ratspräsidentschaft im Jahr 2009 wurde ein neues Mehrjahresprogramm zur Zukunft europäischer Innen- und Sicherheitspolitik der nächsten fünf Jahre beschlossen, das sogenannte Stockholmer Programm.

Aus datenschutzrechtlicher Sicht bleibt das Stockholmer Programm weit hinter seiner eigenen Prioritätensetzung „Wahrung von persönlichen Freiheit“ und „Schutz der Privatsphäre“ zurück. Zum einen sind die Maßnahmen, die der Gewährleistung dieser Schutzgüter dienen sollen, so wenig konkret, dass sie eher wie bloße Lippenbekenntnisse erscheinen, zum anderen enthält der Kommissionsentwurf einen umfangreichen Katalog von eingriffsintensiven Maßnahmen in die vorstehend genannten Schutzgüter. Hierzu gehören zum Beispiel ein elektronisches Registrier- sowie ein Vorabgenehmigungssystem für Ein- und Ausreisen in oder aus der EU und der Aufbau eines europäischen Strafregisterinformationssystems.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder bedarf es weiterer Schritte, um ein ausgewogenes Verhältnis von Sicherheit und Freiheit zu erreichen. Diese Anforderungen hat die 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung formuliert (vergleiche Ziffer 16.11 dieses Berichts).

### 14.3 Urteil des Europäischen Gerichtshofs zum Umfang des datenschutzrechtlichen Auskunftsanspruchs

Werden personenbezogene Daten eines Betroffenen durch eine andere Person oder Stelle erhoben beziehungsweise verwendet, so steht dem Betroffenen nach den Regelungen des Bundesdatenschutzgesetzes (BDSG) grundsätzlich ein Auskunftsanspruch gegenüber dieser verantwortlichen Stelle – Person – zu. Der Auskunftsanspruch erstreckt sich nach § 34 Absatz 1 BDSG grundsätzlich auf die zum Betroffenen gespeicherten Daten, gegebenenfalls auch auf die Herkunft der Daten, auf die Datenempfänger beziehungsweise Datenempfängerkategorien und schließlich auf den Zweck der Speicherung. Ähnliche Auskunftsansprüche sehen aufgrund der entsprechenden europarechtlichen Vorgaben auch die Landesdatenschutzgesetze vor.

Der Europäische Gerichtshof (EuGH) entschied mit Urteil vom 7. Mai 2009, Rechtssache C-553/07, dass sich dieser datenschutzrechtliche Auskunftsanspruch im Fall einer Datenübermittlung über die vorstehend genannten Informationen hinaus auch auf den Inhalt der übermittelten Information erstreckt. Es muss also mitgeteilt werden, welche personenbezogenen Daten im Einzelnen an Dritte weitergegeben wurden. Daneben stellte das Gericht klar, dass der datenschutzrechtliche Auskunftsanspruch auch für die Vergangenheit gilt. Der Anspruch kann also nicht dadurch ausgehebelt werden, dass die verantwortliche Stelle die Information über Datenempfänger und Inhalt der Datenübermittlung nur kurzfristig speichert. Zur Länge

der Aufbewahrungsfrist äußerte sich der Gerichtshof nur insoweit, als er feststellte, das ein angemessener Ausgleich zwischen den Interessen des Betroffenen und denen der verantwortlichen Stelle gefunden werden müsse. Nähere Regelungen zur Aufbewahrungsfrist seien Sache der Mitgliedstaaten der Europäischen Union.

Bundes- wie Landesgesetzgeber sind nunmehr gefordert, die Entscheidung des Europäischen Gerichtshofs in den Datenschutzgesetzen umzusetzen.

### 14.4 SWIFT-Abkommen

Die USA verhandeln mit der Europäischen Union (EU) über ein Abkommen, welches den US-Behörden Zugriff auf Datenströme des Finanzdienstleisters SWIFT (Society for Wordwide Interbank Financial Telecommunication) zum Zwecke der Terrorismusbekämpfung ermöglichen soll. Der Zugriff soll auch auf Daten erfolgen, die keinen Bezug zu den USA haben. Aus verfassungs- und datenschutzrechtlicher Sicht wäre eine solche Zugriffsmöglichkeit höchst bedenklich. Die USA möchten auf Finanzdaten zugreifen, ohne dass gegen die Betroffenen ein hinreichend konkreter Tatverdacht besteht, ohne dass sie an Terroraktivitäten oder an deren Unterstützung mitwirken oder beteiligt waren. Deutschen Sicherheitsbehörden wäre ein solcher Zugriff nicht möglich, da dieser gegen die Verfassung verstoßen würde.

Zudem hätten die Betroffenen kaum Möglichkeiten, sich angemessen gegen die Datenverarbeitung in den USA zu wehren. Die datenschutzrechtlichen Garantien bleiben deutlich hinter den entsprechenden in der EU zurück. Es besteht keine unabhängige Datenschutzkontrolle, und Personen ohne ständigen Wohnsitz in den USA hätten auch kein Recht auf gerichtliche Überprüfung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher in einer Entschließung ihre Erwartung an die Bundesregierung geäußert, dass sie die sensiblen Bankdaten der Bürgerinnen und Bürger wirksam schützt und dem Abkommen nicht zustimmt (vergleiche Ziffer 16.8 dieses Berichts).

Der Rat der europäischen Justiz- und Innenminister hat im November 2009 den Entwurf des Abkommens gebilligt. Das europäische Parlament hat das Abkommen im Februar 2010 abgelehnt und damit vorerst gestoppt. Es ist zu hoffen, dass in den jetzt anstehenden weiteren Verhandlungen mit den USA europäische Datenschutzstandards berücksichtigt werden.

## 15. Datenschutzaudit

### 15.1 Änderung der Datenschutzauditverordnung

Die dem Bremischen Datenschutzgesetz (BremDSG) unterliegenden öffentlichen Stellen können nach § 7 b BremDSG in Verbindung mit § 1 Bremische Datenschutzauditverordnung (BremDSAuditVO) Verfahren einschließlich der dazugehörigen technischen Einrichtungen zum Zwecke der Verbesserung des Datenschutzes und der Datensicherheit prüfen und bewerten lassen, Datenschutzaudit. Die Prüfung und Bewertung wird durch einen Auditor vorgenommen, der auf Vorschlag der öffentlichen Stelle zur Wahrnehmung dieser Aufgabe von der Landesbeauftragten für Datenschutz und Informationsfreiheit zugelassen wurde. Zugelassen wird nur, wer seine fachliche Eignung, persönliche Zuverlässigkeit und Unabhängigkeit für die Tätigkeit als Auditor nachweist. Diesen Nachweis erbringt nach der Bremischen Datenschutzauditverordnung in der Fassung vom 5. Oktober 2004 auch, wer zu einem vergleichbaren Audit im Bund oder einem anderen Land zugelassen wurde. Durch das am 28. Dezember 2009 in Kraft getretene bremische Gesetz zur Umsetzung der EU-Dienstleistungsrichtlinie im Land Bremen und Novellierung weiterer Rechtsnormen (BremGBl. 2009 Seite 535) ist § 1 BremDSAuditVO dahingehend geändert worden, dass den Nachweis auch erbringt, wer zu einem vergleichbaren Audit in einem anderen Mitgliedsstaat der Europäischen Union oder der anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum die Zulassung erhalten hat.

Mit der Regelung zur Berücksichtigung vergleichbarer Audits soll die Prüfung des Vorliegens der Zulassungsvoraussetzungen durch die Landesbeauftragte für Datenschutz und Informationsfreiheit vereinfacht werden. Die Regelung setzt voraus, dass eine Vergleichbarkeit von Audits besteht. Zu unterscheiden ist dabei insbesondere zwischen Verfahrens- und Produktaudits. Sollen Auditierungen nach dem bremischen Datenschutzrecht durchgeführt werden, so handelt es sich um Verfahrens-

audits. Ein abstraktes, verfahrensunabhängiges Produktaudit entspricht den Anforderungen eines Verfahrensaudits nicht (vergleiche 31. Jahresbericht, Ziffer 3.1). Im Hinblick auf die Anerkennung vergleichbarer Audits bei der Zulassung ist daher von uns zunächst die Vergleichbarkeit zu überprüfen. Da bei Audits, die nicht nach dem bremischen Datenschutzrecht erfolgen, häufig lediglich Produktaudits durchgeführt werden, wäre die Vergleichbarkeit in vielen Fällen wohl zu verneinen.

Nach den von uns in Bremen mit der Durchführung von Datenschutzauditierungen gewonnenen Erfahrungen ist auch nur die Beurteilung von Produkten in ihrer technischen Umgebung und ihrem konkreten Einsatzbereich wirklich sinnvoll.

Die benötigten Regelungen zum Datenschutzaudit für die dem Bundesdatenschutzgesetz (BDSG) unterliegenden Stellen fehlen weiterhin. Der vom Bundesminister des Innern in 2008 vorgelegte und von den obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich kritisierte Gesetzentwurf (vergleiche 31. Jahresbericht, Ziffer 21.5) ist nicht verabschiedet worden. Der Bund ist dringend aufgerufen, seiner Gesetzgebungsverpflichtung nach § 9 a BDSG nachzukommen. Benötigt werden angemessene Regelungen, die insbesondere geeignet sind, den Datenschutz in der Wirtschaft zu verbessern.

### 15.2 Re-Auditierung des Verfahrens VERA bei der bremer arbeit gmbH

Die bremer arbeit gmbH (bag) teilte uns im Berichtsjahr mit, dass das von ihr eingesetzte und 2007 erstmals zertifizierte Verfahren VERA (vergleiche 30. Jahresbericht, Ziffer 3.1) einer Re-Auditierung unterzogen werden solle. Nähere Informationen, insbesondere im Hinblick auf die Zulassung des Auditors, über die unsere Behörde entscheidet, und über die Durchführung des Audits erhielten wir zunächst nicht.

Auch bei einer erneuten Auditierung müssen die Vorschriften der Bremischen Datenschutzauditverordnung (BremDSAuditVO) und der hierzu erlassenen Durchführungsbestimmungen eingehalten werden. Wenn sich auch hinsichtlich einer nochmaligen Auditierung durch den selben Auditor das Prüfungs- und Zulassungsverfahren vereinfachen kann, muss trotzdem die Einhaltung der zu beachtenden Bestimmungen gewahrt bleiben. Regelungen, nach denen in solchen Fällen anders verfahren werden kann, gibt es nicht. So bedarf auch bei einer nochmaligen Auditierung das Tätigwerden des Auditors einer vorhergehenden Prüfung und Zulassung durch die Landesbeauftragte für Datenschutz und Informationsfreiheit. Mit der bloßen Mitteilung, das Verfahren VERA befinde sich in der Re-Auditierung, erhielten wir insbesondere keine Informationen darüber, wer das Audit durchführen soll und welchen Umfang und Inhalt es haben soll. Darüber hinaus waren wir auch über Veränderungen des Verfahrens VERA nicht informiert worden. Erst nachdem wir wiederholt auf die zu beachtenden Regelungen hinwiesen und deren Einhaltung verlangten, gelang es, ein den Vorschriften entsprechendes Verfahren zu erreichen. Der von der bag vorgeschlagene Auditor, der bereits das erste Audit durchgeführt hatte, wurde von uns nach einer Prüfung des Vorliegens der notwendigen Voraussetzungen schließlich zugelassen.

## 16. Die Entschließungen der Datenschutzkonferenzen im Jahr 2009

### 16.1 Stärkung der IT-Sicherheit – aber nicht zu Lasten des Datenschutzes

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. Februar 2009)

Das Bundeskabinett hat am 14. Januar 2009 den Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes beschlossen (Bundesrats-Drucksache 62/09). Mit dem Gesetz sollen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) umfassende Befugnisse eingeräumt werden, um Gefahren für die Sicherheit der Informationstechnik des Bundes abzuwehren. Weiter sollen aber zugleich auch das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG) geändert werden.

Angriffe auf die IT-Sicherheit können nicht nur die ordnungsgemäße Abwicklung von Verwaltungsaufgaben beeinträchtigen, sondern auch Gefahren für die Persönlichkeitsrechte der Bürgerinnen und Bürger mit sich bringen. Daher sind Konzepte zu entwickeln und umzusetzen, die sowohl die IT-Sicherheit stärken als auch den Schutz der Privatsphäre gewährleisten.

In weiten Bereichen wurden in der jüngsten Vergangenheit Maßnahmen zur Stärkung der IT-Sicherheit getroffen, die eine detaillierte Registrierung und Auswertung des Nutzerverhaltens und sogar der Inhalte der Kommunikation ermöglichen. Entsprechende Ansätze gibt es nun auch in der Bundesverwaltung. So sieht der Gesetzentwurf vor, dem BSI sehr weitgehende Befugnisse einzuräumen. Kritisch sind insbesondere

1. die Ermächtigung des BSI, die gesamte Sprach- und Datenkommunikation aller Unternehmen, Bürgerinnen und Bürger mit Bundesbehörden ohne Anonymisierung beziehungsweise Pseudonymisierung zu überwachen und auszuwerten (§ 5),
2. die vorgesehene Datenübermittlung an Strafverfolgungsbehörden, insbesondere bei nicht erheblichen Straftaten, wenn sie mittels Telekommunikation begangen werden (§ 5 Absatz 4) und
3. die fehlende Verpflichtung des BSI, Informationen über ihm bekannt gewordene Sicherheitslücken und Schadprogramme zu veröffentlichen und damit Unternehmen, Bürgerinnen und Bürger vor zu (erwartenden) Angriffen (Spionage und Sabotage) zu warnen (§ 7).

Äußerst bedenklich ist darüber hinaus die Regelung, dass im Zweifelsfall allein das Bundesministerium des Innern entscheiden darf, ob Daten dem Kernbereich der privaten Lebensgestaltung zuzuordnen sind und wie damit weiter zu verfahren ist (§ 5 Absatz 6). In solchen Zweifelsfällen sollten diese Daten gelöscht oder einem Richter zur Entscheidung vorgelegt werden.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen zwar grundsätzlich alle Aktivitäten, in den gewachsenen, vernetzten IT-Strukturen des Bundes das Niveau der IT-Sicherheit zu erhöhen. Sie fordern aber auch, dass die zur Risikobegrenzung eingeführten Maßnahmen nicht den Datenschutz der Nutzerinnen und Nutzer beeinträchtigen. Deshalb ist schon bei der Konzeption von IT-Sicherheitsmaßnahmen vorzusehen, dass das erforderliche Sicherheitsniveau nur mit datenschutzgerechten Lösungen gewährleistet wird. Die Datenschutzbeauftragten fordern strengere Sicherheitsstandards und, soweit möglich, die Protokoll- und Inhaltsdaten vor der Auswertung durch das BSI zu anonymisieren beziehungsweise zu pseudonymisieren. Damit ließen sich eine unnötige Registrierung des Nutzerverhaltens und Überwachung von Kommunikationsinhalten vermeiden. Die Auswertung der Daten durch das BSI muss revisionssicher ausgestaltet werden. Der vorgelegte Gesetzentwurf enthält keine solchen Regelungen.

Die Gesetzesänderung des Telemediengesetzes böte öffentlichen und privaten Anbietern von Telemedien die Möglichkeit einer umfassenden Protokollierung des Surfverhaltens ihrer Nutzer im Internet, da sie entsprechend der Gesetzesbegründung weit auslegbar ist. Der Gesetzgeber muss unmissverständlich klarstellen, dass die Erhebung und Auswertung personenbezogener Daten Ultima Ratio ist.

Sowohl die Betreiber der „Netze des Bundes“ als auch die Verantwortlichen für die übergreifenden Netze der Verwaltung in Europa sind aufgefordert, bei allen Maßnahmen zur Stärkung der IT-Sicherheit auch die Privatsphäre und den Datenschutz der Nutzerinnen und Nutzer zu gewährleisten.

### 16.2 Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz

(Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. März 2009)

Datenskandale der letzten Zeit haben deutlich gemacht, dass bei der Verarbeitung von Beschäftigtendaten weder Transparenz noch Rechtssicherheit besteht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, nach jahrelanger Untätigkeit jetzt unverzüglich einen entsprechenden Gesetzentwurf vorzulegen.

Ziel des neuen Beschäftigtendatenschutzgesetzes muss sein, Rechtssicherheit herzustellen, Regelungslücken zu schließen und bereits vorhandene Regelungsaspekte sowie Vorgaben der Rechtsprechung in einem Spezialgesetz zusammenzufassen. Die Konferenz der Datenschutzbeauftragten hält deshalb vor allem folgende Eckpunkte für unverzichtbar:

— Die Regelungen des Beschäftigtendatenschutzgesetzes müssen sowohl für die Beschäftigten der Privatwirtschaft als auch für die Beschäftigten im öffentlichen Dienst gelten.

— Es muss klar geregelt werden, welche Daten Unternehmen und öffentliche Stellen im Rahmen des Einstellungsverfahrens und im weiteren Verlauf des Arbeitslebens über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Es bedarf besonderer Festlegungen im Hinblick auf Gesundheitsdaten (unter anderem zur Frage der Zulässigkeit von Drogen-Screening, psychologischen Testverfahren, ärztlichen Untersuchungen und so weiter).

— Einen umfassenden anlass- und verdachtslosen Datenabgleich darf es nicht geben. Der Zugriff von Kontrollinstanzen, wie zum Beispiel der Innenrevision auf erhobene Personaldaten, bedarf enger gesetzlicher Vorgaben.

— Moderne Informations- und Kommunikationstechnologien dürfen nicht zu lückenlosen Verhaltens- und Leistungskontrollen eingesetzt werden. Da die Nutzung von Telefon, Internet und E-Mail-Diensten nicht mehr aus dem Arbeitsleben wegzudenken ist, sind auch die Voraussetzungen für eine beschäftigtenbezogene Auswertung dieser Kommunikationsmittel eindeutig und restriktiv festzulegen. Dabei ist auch zu regeln, welcher Personenkreis solche Auswertungen durchführen darf und ab welchem Verfahrensstand gegebenenfalls Dritte (zum Beispiel Mitarbeitervertretungen oder Datenschutzbeauftragte) hinzugezogen werden müssen. Auswertungen von Datenbeständen der Zugangs- und Personalinformationssysteme sind strikt zu begrenzen.

— Der Einsatz von Überwachungssystemen, wie zum Beispiel Videokameras und Ortungssystemen, ist auf das unbedingt notwendige Maß zu beschränken und unter Wahrung der Beteiligungsrechte der Mitarbeitervertretungen zulässig. Die Verwendung biometrischer Verfahren bedarf besonders enger Vorgaben.

— Es bedarf der Festlegung der Rechte der Beschäftigten, zum Beispiel im Hinblick auf Auskunfts-, Einsichts-, Widerrufs-, Berichtigungs-, Löschungs- und Schadensersatzansprüche.

— Der Schutz von Persönlichkeitsrechten der in Deutschland tätigen Beschäftigten weltweit agierender Unternehmen oder Konzerne ist sicherzustellen.

— Eine effektive Kontrolle durch die zuständigen Datenschutzbehörden muss gewährleistet werden. Die betrieblichen und behördlichen Datenschutzbeauftragten sind bei allen personaldatenschutzrechtlich relevanten Verfahren und Entscheidungen frühzeitig einzubinden und umfassend zu beteiligen. Ihre Rechte und Befugnisse gegenüber den Mitarbeitervertretungen sind gesetzlich festzulegen.

— Verstöße gegen die Bestimmungen des Beschäftigtendatenschutzgesetzes müssen ein gesetzliches Verwertungsverbot der dadurch gewonnenen Daten nach sich ziehen. Zur Abschreckung bedarf es wirksamer Sanktionen.

### 16.3 Auskunftsanspruch der Steuerpflichtigen im Besteuerungsverfahren gewährleisten

(Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. März 2009)

Das Bundesministerium der Finanzen (BMF) hat mit einer einfachen Verwaltungsanweisung den Auskunftsanspruch der Bürgerinnen und Bürger im Besteuerungsverfahren weitgehend eingeschränkt. Es macht die Auskunftserteilung von einem „berechtigten Interesse“ abhängig, was zu einer Einschränkung des Auskunftsrechts führt.

Die Vorgehensweise des BMF steht im krassen Widerspruch zum Beschluss des Bundesverfassungsgerichts vom 10. März 2008 (1 BvR 2388/03). Danach sind auch von der Finanzverwaltung die Grundrechte auf informationelle Selbstbestimmung und auf effektiven Rechtsschutz zu gewährleisten. Der in § 19 Bundesdatenschutzgesetz (BDSG) verankerte umfassende Auskunftsanspruch findet auch im Besteuerungsverfahren unmittelbare Anwendung.

Es ist inakzeptabel, dass verfassungsrechtlich garantierte Auskunftsrechte der Steuerpflichtigen ausgehebelt werden. Auch die Finanzverwaltung ist an Recht und Gesetz gebunden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass das BMF die Verwaltungsanweisung vom 17. Dezember 2008 unverzüglich

aufhebt. Die Finanzbehörden des Bundes und der Länder sind zu verpflichten, entsprechend der Rechtslage den Auskunftsanspruch zu erfüllen. Die Datenschutzbeauftragten des Bundes und der Länder appellieren zudem an den Bundesgesetzgeber, den Auskunftsanspruch der Steuerpflichtigen durch eine eindeutige Regelung in der Abgabenordnung klarzustellen, die dem § 19 BDSG entspricht.

### 16.4 Defizite beim Datenschutz jetzt beseitigen

(Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. März 2009)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Deutschland auf, endlich die nötigen Konsequenzen aus den nicht mehr abreißenden Datenskandalen zu ziehen. Dazu sind mindestens folgende Schritte geboten:

1. Der Deutsche Bundestag wird aufgefordert, noch in dieser Legislaturperiode die von der Bundesregierung vorgelegten Gesetzentwürfe für erste notwendige Korrekturen des Bundesdatenschutzgesetzes im Bereich der Auskunfteien und des Adresshandels zu verabschieden. Ansonsten verlieren die Bürgerinnen und Bürger das Vertrauen in die Zusagen der Bundesregierung nach den Skandalen des Jahres 2008. Insbesondere mit Adressen darf nur noch mit ausdrücklicher Einwilligung der Betroffenen Handel getrieben werden. Der Entwurf für ein Datenschutzauditgesetz muss gründlich überarbeitet werden, damit dieser notwendige Schritt hin zu einem modernen Datenschutzrecht von der Praxis auch umgesetzt werden kann.
2. Mit Beginn der nächsten Legislaturperiode muss endlich eine grundlegende Modernisierung des Datenschutzrechts in Angriff genommen werden, die bereits zu lange aufgeschoben wurde. Nur so kann das Datenschutzrecht den Herausforderungen der Informationsgesellschaft zu Beginn des 21. Jahrhunderts gerecht werden.
3. Der Einsatz datenschutzfreundlicher Technik muss vorangetrieben und rechtlich verpflichtend vorgeschrieben werden. Darin liegt auch eine Chance für den Wirtschaftsstandort Deutschland in Zeiten der Krise.

### 16.5 Die polizeiliche Datenverarbeitung in INPOL hat keine Rechtsgrundlage

(Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. März 2009)

Die Speicherung von Daten im polizeilichen Informationssystem INPOL durch die Polizeien des Bundes und der Länder ist nur dann rechtmäßig, wenn eine Rechtsverordnung gemäß § 7 Absatz 6 Bundeskriminalamtsgesetz das Nähere über die Art der Daten bestimmt, die in dieser Datei gespeichert werden dürfen. Eine solche Rechtsverordnung existiert nicht. Mit Urteil vom 16. Dezember 2008 (Aktenzeichen 11 LC 229/08) hat das Niedersächsische Oberverwaltungsgericht dies in Bezug auf die Verbunddatei „Gewalttäter Sport“ bekräftigt. Das Urteil ist nicht nur für die Rechtmäßigkeit der Hooligan-Datei bedeutsam, sondern hat Auswirkung auf alle im Rahmen von INPOL geführten Verbunddateien.

Mit der Entscheidung des Gerichts wird die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt. Die vom Bundesministerium des Innern bisher vertretene Auffassung, wonach die Rechtsverordnung keine Zulässigkeitsvoraussetzung für die Datenverarbeitung in den Verbunddateien sei, wird durch die einschlägigen Regelungen nicht gestützt.

Ohne eine derartige Rechtsverordnung ist die Gesamtheit der in Verbunddateien stattfindenden polizeilichen Datenverarbeitungen rechtswidrig. Die Datenschutzbeauftragten von Bund und Länder fordern das Bundesministerium des Innern und die Landesregierungen auf, unverzüglich daraus Konsequenzen zu ziehen und die polizeiliche Datenverarbeitung auf den Prüfstand zu stellen.

### 16.6 Datenschutz beim vorgesehenen Bürgerportal unzureichend

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. April 2009)

Der Gesetzentwurf zur Regelung von Bürgerportalen (Bundesrats-Drucksache 174/09) soll rechtliche Rahmenbedingungen für eine sichere und vertrauenswürdige elektronische Kommunikation zwischen Bürgerinnen und Bürgern und der

Wirtschaft und Verwaltung im lnternet schaffen. Private Anbieter sollen die Portale betreiben, über die der sichere E-Mail-Verkehr De-Mail, eine sichere Dokumentenablage De-Safe und ein Identitätsbescheinigungsdienst abgewickelt werden sollen. Eine solche Infrastruktur stellt hohe Anforderungen an die IT-Sicherheit und den Datenschutz.

Der Gesetzentwurf wird diesen Anforderungen noch nicht gerecht und ist zumindest in folgenden Punkten zu korrigieren:

— Der Entwurf sieht vor, dass nur akkreditierte Anbieterportale betreiben dürfen. Voraussetzung für die Akkreditierung darf nicht allein der Nachweis der technischen und administrativen Sicherheit, sondern muss auch die tatsächliche Einhaltung datenschutzrechtlicher Standards sein. Die dabei zu erfüllenden Mindestanforderungen müssen verbindlich im Gesetz vorgegeben werden. Portalbetreiber sollten zudem erst dann die Akkreditierung erhalten, wenn die Umsetzung dieser Anforderungen durch unabhängige Prüfstellen bescheinigt wurde.

— Die Sicherung der Vertraulichkeit, Integrität und Authentizität von Nachrichteninhalten soll lediglich durch eine Verschlüsselung auf dem Transport zwischen den Diensteanbietern und durch die Sicherung des Zugangs zu den Bürgerportalen erfolgen. Es muss jedoch sichergestellt werden, dass Nachrichten auch bei den Portalbetreibern nicht durch Dritte gelesen oder verändert werden können. Deshalb muss die Kommunikation standardmäßig durch eine Ende-zu-Ende-Verschlüsselung zwischen Absendenden und Empfangenden nach dem Stand der Technik gesichert und nicht nur als Option angeboten werden.

— Das Bürgerportal soll gerade zwischen Bürgerinnnen und Bürgern und Verwaltung eine rechtlich gesicherte Kommunikation ermöglichen. Insbesondere sind über das Bürgerportal förmliche Zustellungen mit den entsprechenden Rechtsfolgen beabsichtigt. Dies darf nur auf Basis einer sicheren Anmeldung erfolgen. Die nach der Gesetzesbegründung ebenfalls mögliche unsichere Anmeldung mit Passwort wird abgelehnt.

— Der Nachweis der Absenderin oder des Absenders soll lediglich durch Anmeldung am Bürgerportal erfolgen. Das ermöglicht Angriffe durch Schadsoftware auf dem Rechner der Nutzenden. So könnten Zugangsdaten beschafft und widerrechtlich dazu verwendet werden, De-Mails zu versenden, empfangene De-Mails zu unterdrücken, zu verzögern und zu verändern oder unberechtigt auf Daten im De-Safe zuzugreifen. Deshalb sind zusätzliche Sicherungsmaßnahmen vorzusehen.

— Die Möglichkeit, eine pseudonyme Bürgerportaladresse zu nutzen, muss – entgegen der Stellungnahme des Bundesrates vom 3. April 2009 – erhalten bleiben. Denn die pseudonyme Nutzung ermöglicht gerade einen sinnvollen Kompromiss zwischen hinreichender ldentifizierbarkeit im Rechtsverkehr und Datenschutz für die Nutzerinnen und Nutzer.

— Die Nutzerinnen und Nutzer müssen bei der Eröffnung des Bürgerportalkontos auf mögliche Rechtsfolgen – etwa zur verbindlichen Kommunikation mit staatlichen Stellen – hingewiesen werden. Die Aufklärungs- und Informationspflichten müssen im Gesetzestext klarer als bislang geschehen gefasst werden. Gleiches gilt für die Feststellung von Identitätsdaten und der Aufdeckung von Pseudonymen.

— Eine Benachteiligung von Bürgerinnen und Bürgern, die über kein Bürgerportalkonto verfügen, muss ausgeschlossen werden. Auch dürfen Bürgerportale nicht dazu führen, dass staatliche Stellen dazu übergehen, bei jeder Inanspruchnahme einer E-Government-Anwendung eine persönliche Identifizierung zu verlangen, selbst wenn dies für die konkrete Dienstleistung nicht erforderlich ist.

— Der Entwurf sieht vor, dass grundsätzliche Fragen der technischen Ausgestaltung der Bürgerportale und der darüber angebotenen Dienste in einer Rechtsverordnung geregelt werden sollen. Dies widerspricht der Rahmenkonzeption des Artikel 80 Grundgesetz und dient auch sonst nicht der Normenklarheit des Gesetzes. Zumindest die grundsätzlichen technisch-organisatorischen Anforderungen an die Eröffnung des Kontos, den Postfach- und Versanddienst, den Speicherplatz, den Identitätsbescheinigungsdienst und das Akkreditierungsverfahren sollten in das Gesetz selbst aufgenommen werden.

— Der Entwurf des Bürgerportalgesetzes sieht jetzt auch vor, dass nicht nur die Datenerhebung, sondern auch die Verarbeitung und Nutzung der erhobenen Daten durch den akkreditierten Diensteanbieter an eine enge Zweckbestimmung gebunden ist. Allerdings ist der pauschale Verweis auf die Regelungen des Bundesdatenschutzgesetzes, des Telemediengesetzes und des Telekommunikationsgesetzes in diesem Zusammenhang zu weitgehend, da so für die Diensteanbieter die Möglichkeit eröffnet wird, die personenbezogenen Daten für Werbung oder Marktforschungszwecke zu nutzen. Die Bürgerinnen und Bürger müssen jedoch sicher sein können, dass ihre Daten ausschließlich zur Teilnahme am Bürgerportal genutzt werden.

### 16.7 Staatsvertrag zum IT-Planungsrat – Datenschutz darf nicht auf der Strecke bleiben

(Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. Oktober 2009)

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

Das Bundesverfassungsgericht hat die besondere Bedeutung der informationellen Selbstbestimmung und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für den Schutz des Persönlichkeitsrechts hervorgehoben. Der in einem Staatsvertrag vorgesehene IT-Planungsrat muss diesen Vorgaben bei der Festlegung verbindlicher Interoperabilitäts- und IT-Sicherheitsstandards für die Datenverarbeitung Rechnung tragen. Für Entscheidungen in grundrechtssensiblen Fragestellungen muss auch der IT-Planungsrat die Zuständigkeit der Parlamente in Bund und Ländern berücksichtigen.

Die im Staatsvertrag vorgesehene vorrangige Verwendung bestehender Marktstandards darf nicht dazu führen, dass Verfahren ohne angemessenen Datenschutz beschlossen werden.

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

### 16.8 Kein Ausverkauf von europäischen Finanzdaten an die USA

(Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. Oktober 2009)

Für Zwecke der Terrorismusbekämpfung verhandeln die USA gegenwärtig mit der Europäischen Union über den Zugriff auf Daten über Finanztransaktionen, die auf SWIFT-Servern (Society for Worldwide Interbank Financial Telecommunication) in Europa gespeichert werden, selbst wenn sie keinerlei Bezug zu den Vereinigten Staaten aufweisen. Besonders kritisch sieht es die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass US-Behörden Zugriffsmöglichkeiten auf Transaktionsdaten anstreben, auch wenn gegen die Betroffenen kein hinreichend konkreter Verdacht besteht, dass sie an Terroraktivitäten oder an deren Unterstützung mitwirken oder beteiligt waren. Ein derartiges Abkommen würde US-Behörden Befugnisse einräumen, die in Deutschland den Sicherheitsbehörden von Verfassungs wegen verwehrt sind.

Ein derartiger weit reichender Eingriff in das Recht auf informationelle Selbstbestimmung weit im Vorfeld des strafrechtlichen Anfangsverdachtes wäre datenschutzrechtlich nicht zu rechtfertigen. Dies wäre auch im Hinblick auf den Vertrauensschutz europäischer Wirtschaftsunternehmen höchst fragwürdig. Der Datentransfer wäre auch deshalb bedenklich, weil die datenschutzrechtlichen Garantien in den USA deutlich hinter den entsprechenden Anforderungen in der Europäischen Union zurückbleiben. Insbesondere besteht dort keine unabhängige Datenschutzkontrolle; Personen ohne ständigen Wohnsitz in den USA haben kein Recht auf gerichtliche Überprüfung der Verwendung ihrer Daten durch US-Behörden.

Im Übrigen bestehen bereits an der Notwendigkeit eines so weit reichenden Zugriffs ausländischer Behörden auf in Europa gespeicherte Daten erhebliche Zwei-

fel. So können Strafverfolgungsbehörden im Rahmen der Rechtshilfe schon heute einzelfallbezogen personenbezogene Daten zur Aufklärung von Terrorismusverdachtsfällen übermitteln.

Schließlich ist zu befürchten, dass eine derartige Regelung über den Zugriff auf SWIFT-Daten Präzedenzwirkung entfalten würde. Zum einen könnten die Vereinigten Staaten mit derselben Begründung Zugriff auf andere in Europa gespeicherte sensible Datenbestände verlangen, etwa die Vorratsdaten der Telekommunikation. Zum anderen wäre es schwer nachvollziehbar, warum die Europäische Union den USA einen so weitgehenden Zugriff auf in Europa gespeicherte Daten einräumt, entsprechende Forderungen anderer Drittstaaten aber zurückweisen sollte.

Die Konferenz erwartet von der Bundesregierung, dass sie die besonders sensiblen Bankdaten der Bürgerinnen und Bürger wirksam schützt und einem Abkommen nicht zustimmt, das eine Datenübermittlung weit unterhalb der Schwelle des strafrechtlichen Anfangsverdachts erlaubt und keine angemessenen datenschutzrechtlichen Standards festlegt.

### 16.9 „Reality-TV" – keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen

(Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. Oktober 2009)

„Reality-TV"-Produktionen über behördliche Einsätze haben in den letzten Jahren erheblich zugenommen. Justiz-, Polizei- und Sozialbehörden scheinen mittlerweile wichtige „Lieferanten" für solche Fernsehsendungen zu sein, die einzelne Bürgerinnen und Bürger bloßstellen und dadurch erheblich in ihre Rechte eingreifen. Das Fernsehpublikum ist dabei, wenn etwa eine Gerichtsvollzieherin versucht, einen Haftbefehl gegen einen Schuldner zu vollziehen – wobei auch schon einmal eine Wohnung zwangsgeöffnet wird – oder wenn die Polizei Verdächtige überprüft oder bei Verkehrsdelikten zur Rede stellt. Es kann vom heimischen Fernsehsessel aus bequem mitverfolgen, ob Betroffene glaubwürdig Einsicht zeigen, unbelehrbar bleiben oder gar ausfällig werden. Aufgrund des Erfolgs derartiger „Unterhaltungssendungen" ist abzusehen, dass die Intensität und die Eingriffstiefe der gezeigten staatlichen Maßnahmen zukünftig immer weiter zunehmen werden.

Presse- und Öffentlichkeitsarbeit sind zwar grundsätzlich notwendig, um die behördliche Aufgabenerfüllung darzustellen und den Informationsanspruch der Öffentlichkeit zu erfüllen. Dabei muss aber das Persönlichkeitsrecht der Betroffenen gewahrt werden, gerade wenn Unterhaltung und Befriedigung von Sensationslust im Vordergrund stehen.

Wird das Fernsehen durch zielgerichtete behördliche Unterstützung in die Lage versetzt, personenbezogene Filmaufnahmen anzufertigen, ist dies rechtlich als Datenübermittlung an private Dritte zu werten. Für einen solchen massiven Eingriff in das Datenschutzgrundrecht der Betroffenen gibt es keine Rechtsgrundlage. Der Staat, der die Betroffenen zur Duldung bestimmter Eingriffsmaßnahmen zwingen kann, ist grundsätzlich nicht befugt, Dritten die Teilnahme daran zu ermöglichen. Auch das Vorliegen einer wirksamen vorherigen Einwilligung der Betroffenen wird regelmäßig zweifelhaft sein. Für eine solche Einwilligung ist es insbesondere notwendig, die betroffene Person rechtzeitig über Umfang, Dauer und Verwendungszwecke der Aufnahmen aufzuklären und auf die Freiwilligkeit seiner Einwilligung hinzuweisen. Angesichts der Überraschungssituation sowie der mit dem staatlichen Eingriff nicht selten verbundenen Einschüchterung ist hier eine besonders sorgfältige Prüfung geboten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb alle Behörden auf, grundsätzlich von der Mitwirkung an solchen „Reality"-Reportagen Abstand zu nehmen.

### 16.10 Aktueller Handlungsbedarf beim Datenschutz – Förderung der Datenschutzkultur

(Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. Oktober 2009)

Zunehmende Überwachung und die ausufernde Verknüpfung von Daten in Staat und Wirtschaft gefährden unser aller Persönlichkeitsrecht. Zusätzliche Herausforderungen ergeben sich aus der technologischen Entwicklung und der Sorglosigkeit der Bürgerinnen und Bürger.

Das aus den 70er Jahren des vorigen Jahrhunderts stammende Datenschutzrecht stellt längst keinen wirksamen Schutz mehr dar. Dies gilt ungeachtet der punktuellen Anpassungen, die das Bundesdatenschutzgesetz seither erfahren hat.

Zu Beginn der neuen Legislaturperiode des Deutschen Bundestags fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Generalrevision des Datenschutzrechts, einschließlich der jüngsten Novellierung zum Adresshandel.

Die Konferenz hält es insbesondere für erforderlich:

— Das Datenschutzrecht an die Herausforderungen neuer Technologien anzupassen und dabei zum Beispiel die Rechte der Betroffenen bei der Nutzung des Internets, insbesondere auf Löschung ihrer Daten, zu verbessern,

— die Integrität und Vertraulichkeit informationstechnischer Systeme zu gewährleisten,

— ein Beschäftigtendatenschutzgesetz zu erlassen und dabei vor allem die Überwachung am Arbeitsplatz effektiv zu begrenzen,

— die Vorratsdatenspeicherung und Onlinedurchsuchung zurückzunehmen,

— die übrigen in den letzten Jahren verschärften Einschränkungen der Grundrechte durch Sicherheitsgesetze des Bundes und der Länder kritisch zu überprüfen,

— auf europäischer und internationaler Ebene auf hohe datenschutzrechtliche Grundstandards hinzuwirken und zum Beispiel den verdachtslosen Zugriff auf Fluggast- und Bankdaten zurückzuweisen,

— im Fall der Einführung der elektronischen Gesundheitskarte die Betroffenenrechte umfassend zu realisieren,

— die Videoüberwachung in Staat und Gesellschaft einzuschränken,

— den Schutz der Meldedaten zu verbessern,

— ein praktikables Datenschutzaudit zu schaffen,

— die Datenschutzaufsichtsbehörden so auszugestalten, dass sie ihre Kontroll- und Beratungsaufgaben unabhängig und effektiv wahrnehmen können.

Datenschutz kann jedoch nicht nur verordnet, er muss auch gelebt werden. Dies setzt eine Datenschutzkultur in Staat, Wirtschaft und Gesellschaft voraus, die gepflegt und weiterentwickelt werden muss.

Die Konferenz spricht sich deshalb dafür aus, den Datenschutz auch als Bildungsaufgabe zu verstehen. Sie fordert Staat, Wirtschaft und Gesellschaft auf, ihre entsprechenden Bildungsanstrengungen zu verstärken. Ziel muss es sein, die Fähigkeit und Bereitschaft der Bürgerinnen und Bürger, insbesondere von Kindern und Jugendlichen, zu fördern, verantwortungsvoll mit ihren eigenen Daten und respektvoll mit den Daten anderer Menschen umzugehen.

### 16.11 Datenschutzdefizite in Europa auch nach Stockholmer Programm

(Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. Oktober 2009)

Die Europäische Union (EU) will im Stockholmer Programm ihre politischen Zielvorgaben zur Entwicklung eines Raums der Freiheit, der Sicherheit und des Rechts für die kommenden fünf Jahre festschreiben. Dazu hat die Kommission der Europäischen Gemeinschaften einen Entwurf vorgelegt.

Zwar erwähnt der Kommissionsentwurf die Wahrung der persönlichen Freiheitsrechte und des Schutzes der Privatsphäre als Prioritäten der Innen- und Sicherheitspolitik in einem „Europa der Bürger“. Schritte wie der geplante Beitritt der Europäischen Union zur Europäischen Menschenrechtskonvention, Aufklärungs- und Informationskampagnen zum Datenschutz und die Förderung und gegebenenfalls Zertifizierung von datenschutzfreundlichen Technologien weisen auch in diese Richtung.

Allerdings bleiben die konkreten Überlegungen für einen verbesserten Datenschutz deutlich hinter den Zielsetzungen für eine verbesserte Sicherheitsarchitektur zurück. Hierzu enthält der Kommissionsentwurf einen umfangreichen Katalog von

zum Teil äußerst eingriffsintensiven Maßnahmen, wie zum Beispiel ein elektronisches Registrier- sowie Vorabgenehmigungssystem für Ein- und Ausreisen in oder aus der Europäischen Union oder den Aufbau eines europäischen Strafregisterinformationssystems. Die ebenfalls angestrebte einheitliche Plattform der Informationsverarbeitung mit beinahe beliebigen Datenverarbeitungsmöglichkeiten gefährdet ohne angemessene Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit die Bürgerrechte.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder bedarf es weiterer Schritte, um in Europa ein ausgewogenes Verhältnis von Sicherheit und Freiheit zu erreichen. Hierzu zählen insbesondere:

— Die Weiterentwicklung des Rahmenbeschlusses 2008/977/JI zu einem harmonisierten und auch für die innerstaatliche Datenverarbeitung verbindlichen Datenschutzrecht, das im Bereich der polizeilichen und justiziellen Zusammenarbeit ein hohes Datenschutzniveau gewährleistet.

— Abschluss von Übereinkommen mit Drittstaaten nur unter der Voraussetzung, dass die zwingenden Datenschutzgrundsätze dort beachtet werden.

— Ein unabhängiges datenschutzrechtliches Beratungs- und Kontrollorgan für alle Bereiche der polizeilichen und justiziellen Zusammenarbeit der EU-Mitgliedstaaten.

— Die Evaluation der vielen auf EU-Ebene beschlossenen sicherheitspolitischen Vorhaben im Hinblick auf ihre Effektivität, den Umfang der mit ihnen verbundenen Grundrechtseingriffe sowie mögliche Überschneidungen der Maßnahmen untereinander, bevor weitere Rechtsakte verabschiedet werden.

— Die Verbesserung von Transparenz und demokratischer Kontrolle bei der Rechtsetzung im Bereich der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene, ungeachtet der Annahme des Vertrages von Lissabon.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich für diese Forderungen – auch unter Berücksichtigung der Kritik des Bundesrates etwa zu der Schaffung von Exekutivbefugnissen für EUROPOL (Europäische Polizeibehörde) und EUROJUST (Europäische Justizbehörde) – im weiteren Verfahren einzusetzen.

### 16.12 Krankenhausinformationssysteme datenschutzgerecht gestalten

(Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. Oktober 2009)

Krankenhausinformationssysteme sind heute zu unverzichtbaren Hilfsmitteln ärztlicher Behandlung in Krankenhäusern geworden. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist jederzeit, ortsungebunden und sekundenschnell möglich und bietet damit die Grundlage für effiziente Behandlungsentscheidungen. Diesen Vorteilen stehen allerdings erhebliche Datenschutzrisiken gegenüber. Die Möglichkeiten für Klinikpersonal, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen und privat zu nutzen, sind groß. Prüfungen der Datenschutzaufsichtsbehörden und bekannt gewordene Missbrauchsfälle belegen dies.

Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln.

Die Konferenz der Datenschutzbeauftragten fordert daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Darüber hinaus fordert die Konferenz, dass Patienten nachvollziehen können, wer auf ihre Daten tatsächlich zugegriffen hat. Das ist Teil des Menschenrechts auf Achtung des Privatlebens nach Artikel 8 der Europäischen Menschenrechtskonvention, wie der Europäische Gerichtshof für Menschenrechte klargestellt hat. Durch Protokollierung ist zu gewährleisten, dass eine nachträgliche Überprüfung der Zugriffe auf ihre Zulässigkeit möglich ist. Die Systeme müssen behandlungs- und patientenbezogen den technischen Zugriff gemäß den rechtlichen Befugnissen ermöglichen.

Die Krankenhäuser sind in der Pflicht, datenschutzgerechte Systeme einzusetzen. Die Software-Hersteller sind gehalten, entsprechende Systeme anzubieten.

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

### 17.1 Telemarketing bei NGOs

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich vom 23. bis 24. April 2009 in Schwerin)

Auch die sogenannten NGOs (non governmental organization), also nicht staatliche Organisationen, die gemeinnützig oder auch als Interessenverbände tätig sind, haben in den letzten Jahren zunehmend damit begonnen, Telefonmarketing zu betreiben. Beworben werden insbesondere Personen, die schon einmal für die jeweilige NGO gespendet haben. Wenn der Spender seine Telefonnummer in den früheren Kontakten nicht angegeben hat, wird dieses Datum mit Hilfe des Telefonbuches oder einer Telefon-CD ermittelt.

Die Aufsichtsbehörden erklären, dass auch NGOs ohne Einwilligung der Betroffenen nicht zu telefonischer Werbung berechtigt sind. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu diesem Zweck ist ohne Einwilligung rechtswidrig.

### 17.2 Datenschutzrechtliche Aspekte des Mitarbeiter-Screenings in international tätigen Unternehmen

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich vom 23. bis 24. April 2009 in Schwerin)

Viele Unternehmen sind dazu übergegangen, ihre Mitarbeiter gegenüber Listen abzugleichen, die terrorverdächtige Personen und Organisationen enthalten. Insbesondere Unternehmen, die internationalen Konzernen angehören, werden von ihren teilweise in Drittländern ansässigen Muttergesellschaften hierzu aufgefordert. Letztere stellen auch darüber hinaus gehende Listen zum Beispiel mit gesuchten Personen zur Verfügung, die aufgrund nationaler Vorschriften in den Drittländern einzusetzen sind.

Nach § 4 Absatz 1 Bundesdatenschutzgesetz (BDSG) sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Zwar kann § 28 Absatz 1 BDSG eine Rechtsgrundlage im Sinne des BDSG sein, diese Vorschrift kann jedoch für ein Screening nicht herangezogen werden. Der Abgleich mit den Listen dient nicht dem Vertragsverhältnis. Eine Abwägung der Unternehmens- und Betroffeneninteressen führt zu überwiegenden schutzwürdigen Interessen der Betroffenen. Dies gilt insbesondere vor dem Hintergrund, dass die Rechtsstaatlichkeit des Zustandekommens der Listen nachvollziehbar und gesichert sein muss, sowie Rechtsschutzmöglichkeiten bestehen müssen. Angesichts der fehlenden Freiwilligkeit einer solchen Erklärung im Arbeitsverhältnis kann auch das Vorliegen einer Einwilligung eine konkrete Rechtsgrundlage nicht ersetzen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich stellen daher fest, dass im Geltungsbereich des Bundesdatenschutzgesetzes lediglich solche Listen verwendet werden dürfen, für die eine spezielle Rechtsgrundlage im Sinne des § 4 Absatz 1 BDSG vorliegt.

In diesem Zusammenhang weisen die obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich auch auf die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. bis 17. März 2006 in Magdeburg hin.

### 17.3 Unzulässige Übermittlungen von Passagierdaten an britische Behörden verhindern

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 13. Juli 2009)

Der Düsseldorfer Kreis stellt fest, dass die Übermittlung von Passagierdaten (Ausweis- und Reservierungsdaten) durch Fluggesellschaften in Deutschland an die bri-

tischen Zoll- und Sicherheitsbehörden für innereuropäische Flüge unzulässig ist. Die Bundesregierung wird gebeten, entsprechenden Forderungen der britischen Behörden entgegenzutreten.

Großbritannien verlangt im Rahmen des sogenannten eBorders-Projektes die Erhebung und Übermittlung von Ausweisdaten der Reisenden für innereuropäische Flüge von und nach Großbritannien und die Übermittlung von Daten aus den Reservierungsdatenbanken der Fluggesellschaften. Die britischen Behörden berufen sich bei ihrer Forderung auf die britische Gesetzgebung für Grenzkontrollen. Diese durch das eBorders-Projekt konkretisierte Gesetzgebung berührt einerseits den freien Reiseverkehr in der Europäischen Union. Andererseits bezieht sie sich auf Sachverhalte, die nicht alleine in der Regelungskompetenz des britischen Gesetzgebers liegen, weil sie Datenerhebungen in anderen Mitgliedstaaten der Europäischen Union vorschreibt und Übermittlungen aus Datenbanken verlangt, die sich in anderen Mitgliedstaaten befinden.

Die Übermittlung von Reservierungsdaten der Passagiere an britische Grenzkontrollbehörden, die sich in Datenbanken der verantwortlichen Fluggesellschaften in Deutschland befinden, ist nach deutschem Recht nicht erlaubt. Insbesondere enthält das Bundesdatenschutzgesetz (BDSG) keine Rechtsgrundlage, auf die die Fluggesellschaften die geforderte Übermittlung stützen könnten.

Bereits bei entsprechenden Forderungen der USA, Kanadas und Australiens bestand in Europa Konsens, dass die Übermittlung nicht zur Erfüllung der Flugreiseverträge erfolgt (§ 28 Absatz 1 Satz 1 Nummer 1 BDSG) und wegen der Zwangslage nicht auf eine Einwilligung (§ 4 a BDSG) der Reisenden gestützt werden kann. Sie dient auch nicht den berechtigten Interessen der Fluggesellschaften, die selbst den Forderungen der britischen Behörden entgegentreten, weil sie sich als Reiseunternehmen und nicht als Gehilfen der Grenzkontrollbehörden verstehen. Außerdem besteht ein überwiegendes Interesse der Flugreisenden daran, dass eine Übermittlung ihrer Daten unterbleibt, solange die Vereinbarkeit der britischen Forderung mit vorrangigem europäischen Recht nicht geklärt ist (§ 28 Absatz 1 Satz 1 Nummer 2 BDSG). Schließlich kann eine solche verdachts- oder gefahrunabhängige Übermittlung der Daten aller Reisenden für Sicherheitszwecke nicht auf § 28 Absatz 3 Satz 1 Nummer 2 BDSG gestützt werden, da diese Vorschrift das Vorliegen einer konkreten Gefahr oder Straftat voraussetzt.

Die Übermittlung der Reservierungsdaten ist außerdem verfassungsrechtlich bedenklich und auch fraglich im Hinblick auf die Vereinbarkeit mit der Europäischen Menschenrechtskonvention.

Was die Erhebung von Ausweisdaten anbelangt, gehen die britischen Behörden über die Europäische Richtlinie 2004/82/EG über die Verpflichtung von Beförderungsunternehmen, Angaben über beförderte Personen zu übermitteln, insoweit hinaus, als Daten auch für innereuropäische Flüge erhoben werden sollen. Die Europäische Kommission prüft zurzeit, ob diese einseitige Regelung eine Verletzung der Richtlinie 2004/82/EG darstellt. Jedenfalls dürfte eine solche Maßnahme im Hinblick auf die Freizügigkeit in der Europäischen Union kontraproduktiv sein. Der Düsseldorfer Kreis erwartet, dass die Erhebung und Übermittlung von Pass- und Ausweisdaten für innereuropäische Flüge bis zu einer Bewertung durch die Europäische Kommission unterbleiben.

### 17.4 Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz in nicht öffentlichen Bereich am 22. Oktober 2009)

Häufig holen Vermieter Informationen bei Auskunfteien über die Bonität von Mietinteressenten ein, bevor sie Wohnraum vermieten. Hierfür gelten folgende Anforderungen:

1. Vermieter dürfen erst dann eine Auskunft zu einem Mietinteressenten einholen, wenn der Abschluss des Mietvertrags mit diesem Bewerber nur noch vom positiven Ergebnis einer Bonitätsprüfung abhängt.
2. Es dürfen nur folgende Datenkategorien nach Darlegung eines konkreten berechtigten Interesses an Vermieter übermittelt werden, sofern diese Daten zulässigerweise an die Auskunftei übermittelt bzw. von dieser erhoben wurden:
   - Informationen aus öffentlichen Schuldner- und Insolvenzverzeichnissen;

— sonstige Daten über negatives Zahlungsverhalten, bei denen

  — die dem jeweiligen Eintrag zugrunde liegende Forderung noch offen ist oder – sofern sie sich zwischenzeitlich erledigt hat – die Erledigung nicht länger als ein Jahr zurückliegt und

  — eine Bagatellgrenze von insgesamt 1.500 Euro überschritten wird.

3. Die Übermittlung von Scorewerten an Vermieter ist unzulässig, sofern darin andere als die unter Nummer 2 erwähnten Daten verwendet werden.

4. Vermieter dürfen weitergehende als die unter 2. genannten Daten grundsätzlich auch nicht im Wege einer Einwilligung oder einer Selbstauskunft des Mietinteressenten von einer Auskunftei erheben.

**Hintergrund:**

Nach § 29 Absatz 2 Nummer 1 a Bundesdatenschutzgesetz (BDSG) ist die Erteilung von Bonitätsauskünften nur zulässig, wenn der Vermieter ein berechtigtes Interesse hieran hat und wenn kein Grund zu der Annahme besteht, dass der betroffene Mietinteressent ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Da Vermieter mit dem Abschluss eines Mietvertrages das Risiko eingehen, dass ein Mieter aufgrund von Zahlungsunfähigkeit oder -unwilligkeit den Mietzins oder Nebenkosten nicht begleicht, erkennen die Aufsichtsbehörden an, dass Vermieter aufgrund dieses finanziellen Ausfallrisikos grundsätzlich ein berechtigtes Interesse an einer Bonitätsauskunft über einen Mietinteressenten haben.

Bei der erforderlichen Abwägung sind allerdings auch die schutzwürdigen Belange der Mietinteressenten im Hinblick auf die Bedeutung der Wohnung für die Lebensgestaltung zu berücksichtigen. Ferner ist zu beachten, dass Mietkautionen in Höhe von bis zu drei Monatsmieten, das Vermieterpfandrecht und die bei nachträglicher Zahlungsunfähigkeit vielfach in die Zahlungspflicht eintretenden Sozialbehörden das finanzielle Risiko der Vermieter teilweise reduzieren.

Schließlich ist zu berücksichtigen, dass Auskunfteien an Vermieter nur Bonitätsdaten übermitteln dürfen, die eindeutig Rückschlüsse auf Mietausfallrisiken zulassen. Da das Zahlungsverhalten je nach Vertragsverhältnis unterschiedlich sein kann und teilweise auch ist, lassen zu spät oder nicht gezahlte Kleinbeträge etwa aus Handyverträgen und Internetgeschäften nicht unbedingt einen spezifischen Rückschluss auf die Zahlungsmoral bei Mietverträgen zu.

Aufgrund dieser Erwägungen haben die Aufsichtsbehörden nach Gesprächen mit den Auskunfteien und der Wohnungswirtschaft bereits im Jahr 2004 festgestellt, dass Auskunfteien keine uneingeschränkten Bonitätsauskünfte über Mietinteressenten erteilen dürfen. Vorzuziehen – so der damalige Beschluss – seien branchenspezifische Auskunftssysteme, die auf gesicherte Daten zu negativem Zahlungsverhalten aus öffentlichen Schuldnerverzeichnissen und dem Mietbereich beschränkt sind.

Die eingangs dargelegten Anforderungen berücksichtigen wesentliche Kritikpunkte der Wohnungswirtschaft und der Auskunfteien. So enthält der nunmehr definierte Katalog weder eine Beschränkung auf Daten aus dem Mietbereich noch eine Beschränkung auf titulierte Negativmerkmale. Eine derartige Beschränkung hatten mehrere Aufsichtsbehörden bislang auf Grundlage des Beschlusses aus dem Jahr 2004 gefordert und gegenüber so genannten Mieterwarndateien auch durchgesetzt.

Selbstverständlich dürfen nur Daten, die zulässigerweise bei der Auskunftei eingemeldet wurden, von dieser an Vermieter übermittelt werden. Das heißt, die allgemeinen Einmeldevoraussetzungen, die der Gesetzgeber im neuen § 28 a BDSG präzisiert hat und die bereits bisher von den Aufsichtsbehörden gefordert wurden, müssen eingehalten werden.

Die Bagatellgrenze von 1.500 Euro errechnet sich aus drei Monatsmieten der durchschnittlichen Kaltmiete. Nach der jüngsten Einkommens- und Verbrauchsstichprobe des Statistischen Bundesamtes beträgt sie monatlich 515 Euro.

Auch wenn die Speicher- bzw. Überprüfungsfrist der Auskunfteien bei Forderungen, die nach der Einmeldung beglichen wurden, drei Jahre beträgt (§ 35 Absatz 2 Nummer 4, 2. Halbsatz BDSG neu), ist ein berechtigtes Interesse von Vermietern an der Kenntnis solcher Daten nur für ein Jahr anzuerkennen. Daher ist auch nur innerhalb dieses Zeitraums eine Übermittlung an Vermieter zulässig. Ansonsten wäre dem Schuldner die Eingehung eines Mietverhältnisses unvertretbar erschwert.

Die Unzulässigkeit der Übermittlung von Scorewerten an Vermieter ergibt sich daraus, dass abgesehen von der allgemeinen Problematik der Scoreberechnung im Mietbereich die besondere Problematik besteht, dass die spezifischen Einschränkungen unterlaufen würden, wenn eine Scoreberechnung mit Daten erfolgte, die über den unter Nummer 2 genannten Katalog hinausgehen.

Die Einforderung von unbegrenzten Selbstauskünften oder Einwilligungen zur Einholung weit gefasster Auskünfte vom Mietinteressenten würde eine Umgehung der sich aus der Abwägung nach § 29 BDSG ergebenden gesetzlichen Begrenzungen darstellen, was demzufolge nicht zulässig ist.

Die bisherige Praxis der Auskunfteien entsprach den hier gestellten Anforderungen nicht beziehungsweise nicht in ausreichendem Maße. Obwohl den Auskunfteien ausdrücklich die Möglichkeit eingeräumt wurde, gegebenenfalls alternative Lösungen zu den im Beschluss genannten Anforderungen zu entwickeln, die auf das jeweilige Geschäftsmodell der Auskunfteien und deren speziellen Datenbestand zugeschnitten sind, haben die Auskunfteien diese Möglichkeit bislang nicht genutzt.

Die Aufsichtsbehörden haben in Gesprächen mit den Auskunfteien angekündigt, dass sie bei datenschutzwidrigen Übermittlungen gegebenenfalls aufsichtsrechtliche Maßnahmen ergreifen werden.

### 17.5 Keine Internetveröffentlichung sportgerichtlicher Entscheidungen

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich vom 26. bis 27. November 2009 in Stralsund)

Entgegen der Auffassung des Oberlandesgerichts Karlsruhe in seinem Urteil vom 30. Januar 2009 gehen die zuständigen Aufsichtsbehörden in Anwendung des Bundesdatenschutzgesetz davon aus, dass die uneingeschränkt zugängliche Veröffentlichung von sportgerichtlichen Entscheidungen im Internet unzulässig ist. Entsprechendes gilt auch für die Veröffentlichung von personenbezogenen Sperrlisten.

Eine Veröffentlichung in geschlossenen Benutzergruppen ist zulässig, wenn gewährleistet ist, dass in den Vereinen nur zuständige Personen zugreifen können. Soweit der Personenbezug nicht erforderlich ist, sind sportgerichtliche Entscheidungen zu anonymisieren.

Bei der mit der Veröffentlichung im Internet verbundenen Datenübermittlung an Dritte wird der Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen meist deswegen als besonders gravierend empfunden, weil hierdurch nicht nur ein weltweiter Zugriff auf die Daten, sondern darüber hinaus vor allem eine elektronische Recherchierbarkeit ermöglicht wird, welche auch zur Erstellung eines Persönlichkeitsprofils genutzt werden kann.

Der beabsichtigten „Prangerwirkung“ mit Abschreckungsfunktion könnte bereits dadurch Genüge getan werden, dass entsprechende Ahndungen organisationsintern beziehungsweise verbandsintern in zugriffsgeschützten Internetforen „für die, die es angeht“, publizieren würden. Die intendierte Information der Öffentlichkeit über das Vorgehen gegen Rechtsverstöße könnte ohne Personenbezug im Rahmen einer Ahndungsstatistik erfolgen.

### 17.6 Gesetzesänderung bei der Datenverwendung für Werbezwecke

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich vom 26. bis 27. November 2009 in Stralsund)

Vom 1. September 2009 an gelten nach § 28 Absatz 3 Bundesdatenschutzgesetz neue Datenschutzregelungen bei der Datenverwendung für Werbezwecke. Diese Regelungen gelten spätestens ab dem 31. August 2012, jedoch sofort für Daten, die nach dem 1. September 2009 erhoben oder von einer Stelle erstmalig gespeichert werden.

Die Datenschutzaufsichtsbehörden weisen darauf hin, dass für Daten, deren erstmalige Speicherung nicht eindeutig erkennbar ist, die neuen Regelungen angewendet werden. Sie weisen weiterhin darauf hin, dass eine Übermittlung für Werbezwecke nur zulässig ist, wenn Herkunft der Daten und Empfänger gespeichert werden und eine Gruppenauswahl nach einem Merkmal erfolgt (Listenübermittlung). Bei der Werbemaßnahme muss die erstmalig erhebende Stelle den Adressaten mitgeteilt werden. Die bisher weit verbreitete Praxis der Übermittlung von nach mehr als einem Merkmal selektierten Adressen ist unzulässig, wenn keine Einwilligung vorliegt.

### 17.7 Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich vom 26. bis 27. November 2009 in Stralsund)

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

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

Im Einzelnen sind folgende Vorgaben aus dem TMG zu beachten:

— Den Betroffenen ist eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen. Derartige Widersprüche sind wirksam umzusetzen.

— Die pseudonymisierten Nutzungsdaten dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Sie müssen gelöscht werden, wenn ihre Speicherung für die Erstellung der Nutzungsanalyse nicht mehr erforderlich ist oder der Nutzer dies verlangt.

— Auf die Erstellung von pseudonymen Nutzungsprofilen und die Möglichkeit zum Widerspruch müssen die Anbieter in deutlicher Form im Rahmen der Datenschutzerklärung auf ihrer Internetseite hinweisen.

— Personenbezogene Daten eines Nutzers dürfen ohne Einwilligung nur erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Jede darüber hinausgehende Nutzung bedarf der Einwilligung der Betroffenen.

— Die Analyse des Nutzungsverhaltens unter Verwendung vollständiger IP-Adressen (einschließlich einer Geolokalisierung) ist aufgrund der Personenbeziehbarkeit dieser Daten daher nur mit bewusster, eindeutiger Einwilligung zulässig. Liegt eine solche Einwilligung nicht vor, ist die IP-Adresse vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist.

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

## 18. Die Europäische und die Internationale Datenschutzkonferenz

Bei der Europäischen und der Internationalen Konferenz der Datenschutzbeauftragten, an denen wir nicht teilnahmen, standen in erster Linie grundsätzliche Fragestellungen des Datenschutzes auf der Tagesordnung.

**Europäische Datenschutzkonferenz:**

Die Europäische Datenschutzkonferenz fand am 23. und 24. April 2009 in Edinburgh statt. Hier wurde unter anderem die „Erklärung zur Führungsrolle und Zukunft des Datenschutzes in Europa“ verabschiedet. Diese betont die Notwendigkeit von hohen Datenschutzstandards in allen Lebensbereichen. Zudem wird in der Erklärung eine Verbesserung der Datenschutzgesetzgebung gefordert.

**Internationale Datenschutzkonferenz:**

Die 31. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre, die vom 4. bis 6. November 2009 in Madrid stattfand, hat sich mit der Verbesserung und Vertiefung der internationalen Zusammenarbeit befasst. Weiterer Schwerpunkt war der Datenschutz am Arbeitsplatz.

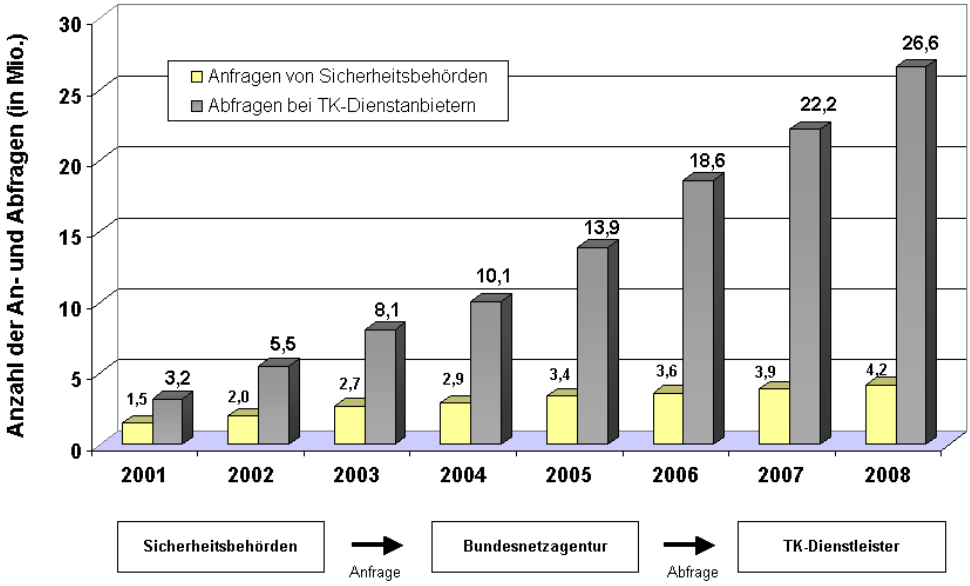
Die Entschließungen der Europäischen und Internationalen Datenschutzkonferenz stehen auf der Internetseite des Bundesbeauftragten für Datenschutz und Informationsfreiheit unter:

http://www.bfdi.bund.de/cln_134/DE/Entschließungen/entschließungen_node.html

zur Verfügung.

## 19. Anhang

### 19.1 Automatisiertes Auskunftsverfahren gemäß § 112 Telekommunikationsgesetz




Sicherheitsbehörden erhalten gemäß § 112 Telekommunikationsgesetz (TKG) über die Bundesnetzagentur von Telekommunikationsdienstanbietern Auskünfte aus deren Kundendateien (Namen und Anschrift der Inhaber von Rufnummern). Der Kreis der ins automatisierte Verfahren eingebundenen Behörden und verpflichteten Unternehmen wurde im Laufe der Jahre stetig vergrößert. Im abgebildeten Diagramm ist die Entwicklung beim automatisierten Auskunftsverfahren gemäß § 112 TKG im Zeitraum 2001 bis 2008 dargestellt.

### 19.2 Liste des verfügbaren Informationsmaterials

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

## 19.3 Index

Druck: Anker-Druck Bremen