**BREMISCHE BÜRGERSCHAFT** **Drucksache 18 / 805**
Landtag 08. 03. 13
18. Wahlperiode

# 35. Jahresbericht der Landesbeauftragten für Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats meinen Bericht über das Ergebnis der Tätigkeit im Jahr 2012. Redaktionsschluss für die Beiträge war der 31. Dezember 2012.

**Dr. Imke Sommer**
Die Landesbeauftragte für Datenschutz und Informationsfreiheit
der Freien Hansestadt Bremen

**Inhaltsverzeichnis**

# 1. Einleitung

## 1.1 Nachruf auf die Gesichtserkennung bei facebook

Liebe Menschen im Land Bremen,
haben Sie bemerkt, dass facebook die automatische Gesichtserkennungsfunktion abgeschaltet hat? Im letzten Jahresbericht hatte ich über diese Funktion berichtet (vergleiche 34. Jahresbericht, Ziffern 1.2 und 1.3). Die Gesichtserkennung in dem sozialen Netzwerk sollte es erleichtern, Menschen auf Fotos mit ihrem Namen zu versehen. Hierfür wurden von facebook automatisch für jede Nutzerin und jeden Nutzer Muster angelegt, die auf biometrischen Daten beruhten. So baute facebook im Hintergrund eine der wahrscheinlich größten Datenbanken mit biometrischen Daten auf. Von allen bis Juli 2012 registrierten Nutzerinnen und Nutzern hatte facebook biometrische Gesichtsmodelle erstellt, ohne dass die Nutzerinnen und Nutzer genaue Informationen über das Verfahren der Gesichtserkennung bekommen oder eingewilligt hätten.

Der Verzicht facebooks auf diese Funktion der automatischen Gesichtserkennung, die gegen deutsches und europäisches Datenschutzrecht verstieß, vollzog sich in zwei Etappen. Im Sommer 2012 erklärte das Unternehmen, ab Juli 2012 würde auf die Erfassung von biometrischen Daten neuer Nutzerinnen und Nutzer verzichtet werden. Weitere Anpassungen lehnte das Unternehmen zu diesem Zeitpunkt ab. Am 21. September 2012 erklärte facebook dann aber, das Verfahren der automatischen Gesichtserkennung in Europa nicht mehr weiterzuverfolgen und die entstandene Datenbank mit den biometrischen Daten der europäischen Nutzerinnen und Nutzer zu löschen.

Dieser Entscheidung facebooks waren viele Maßnahmen europäischer Datenschutzeinrichtungen vorausgegangen, die sich mit unterschiedlichen Methoden gegen die rechtswidrige Anwendung wandten. Mein hamburgischer Kollege hatte bereits im Dezember 2011 ein Verwaltungsverfahren eingeleitet, in dem facebook zu einer bevorstehenden Anordnung angehört wurde. Die Artikel-29-Gruppe, in die jeder Mitgliedsstaat der Europäischen Union eine Vertreterin oder einen Vertreter der Datenschutzbehörden entsendet, hatte im März 2012 ein kritisches „Workingpaper“ („Arbeitsdokument“) zur Gesichtserkennung veröffentlicht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Deutschland hatte in ihrer Entschließung „Datenschutz bei sozialen Netzwerken jetzt verwirklichen!“ (vergleiche 34. Jahresbericht, Ziffer 21.7) klargestellt, dass sich die Anbieter von sozialen Netzwerken, die auf den europäischen Markt zielen, auch dann an europäische Datenschutzstandards halten müssen, wenn sie ihren Geschäftssitz außerhalb Europas haben. Ein österreichischer Student hatte im August 2011 mehrere Beschwerden über facebook beim irischen Datenschutzbeauftragten eingereicht. Noch kurz vor der Rücknahme des Gesichtserkennungsverfahrens hatte der irische Datenschutzbeauftragte von facebook gefordert, ausreichende Informationen über das Verfahren für Nutzerinnen und Nutzer bereitzustellen sowie die Datenverwertungsrichtlinien anzupassen. Mein Kollege aus Schleswig-Holstein kündigte in einer Pressemitteilung am 21. September 2012 in Sachen Gesichtserkennungsfunktion ein unmittelbar bevorstehendes gemeinsames Vorgehen mit meinem Kollegen aus Rheinland-Pfalz und uns aus Bremen an. Wir wollten, wie in Hamburg, ein Anhörungsverfahren beginnen, das auf die Anordnung zur Abschaltung der Gesichtserkennungsfunktion für die Mitglieder des Netzwerkes facebook in unseren jeweiligen Bundesländern zielte. Die sich in Hamburg an das Anhörungsverfahren anschließende Anordnung wurde am 21. September 2012 erlassen und kreuzte sich insofern mit der Erklärung facebooks, auf das Gesichtserkennungsverfahren vollständig zu verzichten. Der Hamburgische Datenschutzbeauftragte verpflichtete facebook damit sicherzustellen, die automatische Gesichtserkennung nur bei denjenigen Nutzerinnen und Nutzern einzusetzen, die zuvor darin ausdrücklich und informiert eingewilligt hatten, den Nutzerinnen und Nutzern ausreichende Informationen zu Funktion und Risiken der automatischen Gesichtserkennung zur Verfügung zu stellen und alle biometrischen Muster und Informationen zu löschen, die bisher ohne Einwilligung der betroffenen Nutzerinnen und Nutzer erfasst worden waren.

Zeigt diese Aufzählung die Macht der europäischen Datenschutzinstitutionen? Wahrscheinlich eher nicht. Sie zeigt aber, dass das Zusammenwirken europäischer Datenschutzeinrichtungen schon auf der Grundlage der heutigen europäischen Rechtslage Erfolge haben kann. Welchen Einfluss unsere Aktivitäten auf die Ent-

scheidung des Unternehmens facebook hatten, lässt sich nicht genau feststellen. Jedenfalls spricht vieles dafür, dass es für das Erreichte sehr günstig war, dass sich die Initiativen zur Durchsetzung des Datenschutzes unterschiedlicher Instrumente bedienten und aus unterschiedlichen europäischen Ländern kamen.

Der geschilderte Fall der Durchsetzung einer datenschutzrechtlichen Forderung belegt sehr gut, dass Forderungen in einzelnen Mitgliedsstaaten, die auf ein hohes Datenschutzniveau gerichtet sind, zur Ausdehnung dieses Datenschutzniveaus auf ganz Europa führen. Der Grund hierfür wird sein, dass es für global agierende Unternehmen in wirtschaftlicher Hinsicht, aber wegen der Vernetzung der Nutzerinnen und Nutzer in Europa auch aus fachlicher Sicht nicht sinnvoll ist, für den Markt der Europäischen Union national unterschiedliche Anwendungen zu programmieren. Ein höheres europäisches Mindestdatenschutzniveau hätte diesen datenschutzrechtlichen Erfolg mit Sicherheit beschleunigt. Vielleicht wäre der datenschutzwidrige Zustand sogar gar nicht erst eingetreten. Und das bringt mich zum großen datenschutzrechtlichen Thema des Berichtsjahres.

### 1.2 Der Kommissionsvorschlag für eine Datenschutz-Grundverordnung

Die EU-Kommission (EU = Europäische Union) hat im Februar 2012 Entwürfe für einen europäischen Rechtsrahmen für den Datenschutz vorgelegt. Dazu gehört an erster Stelle eine Verordnung, die die gegenwärtig geltende EU-Datenschutzrichtlinie ablösen soll.

Die Diskussion um den Vorschlag der Europäischen Kommission wird in Deutschland – wie es das vorgeschlagene Kürzel „Datenschutz-Grundverordnung“ nahe legt – als Diskussion über den Datenschutz in Europa geführt. Dass dies eine Verkürzung darstellt, zeigt schon der vollständige Titel des Kommissionsvorschlages für eine Verordnung „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“. Also, um es auf den Punkt zu bringen: Nicht überall dort, wo Datenschutz-Grundverordnung drauf steht, ist allein Datenschutz drin. Und damit nicht genug: Bei genauerem Hinsehen zeigt sich, dass der Kommissionsentwurf das Schutzziel des freien Datenverkehrs im Vergleich zum Schutzziel Datenschutz sogar privilegiert.

Dass der Kommission das Ziel des freien Datenverkehrs sehr am Herzen liegt, zeigt schon die Einbettung des Kommissionsvorschlages in ihr Projekt der „digitalen Agenda“, die unter anderem einen „digitalen Binnenmarkt“ anstrebt. Als Ziele des Kommissionsvorschlages werden in diesem Zusammenhang die Stärkung der Privatheitsrechte im Online-Bereich und die Ankurbelung der europäischen digitalen Wirtschaft genannt. Das Verhältnis dieser beiden Ziele erschließt sich, wenn die Kommission die Problemlage beschreibt: Die kritische Überprüfung der europäischen Datenschutzregelungen sei erforderlich, weil die Konsumentinnen und Konsumenten bei Online-Aktivitäten wenig Vertrauen hätten, dass ihre Privatheit beachtet werde. Mangelndes Vertrauen bedeute weniger Online-Geschäft, es bremse das Wachstum der europäischen Online-Wirtschaft.

Diese Aussagen zeigen, dass die Kommission den Datenschutz vorrangig als Instrument zur Herstellung des digitalen Binnenmarktes versteht. Das auf den Datenschutz bezogene Ziel wird gerade nicht als die größtmögliche Verwirklichung des Datenschutzgrundrechtes gesehen. Als Ziel wird vielmehr die Herstellung einer Situation beschrieben, in der die Grundrechtsträgerinnen und Grundrechtsträger das subjektive Empfinden haben, das Grundrecht werde geschützt, weil sie erst dann Konsumentscheidungen treffen, die der europäischen Online-Wirtschaft zugute kommen.

Die Frage, ob das Vertrauen der Konsumentinnen und Konsumenten dahinein, dass ihre personenbezogenen Daten im Internet geschützt sind, tatsächlich gerechtfertigt ist, erscheint nach dieser Argumentation zweitrangig. Dieser Parteinahme des Kommissionsvorschlages für das Schutzziel des freien Datenverkehrs sind in der Diskussion aus Datenschutzsicht Forderungen entgegengestellt worden, die dem Datenschutzgrundrecht ein größeres Gewicht verschaffen würden, als dies im Kommissionsentwurf bislang vorgesehen ist. So hat sich beispielsweise die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer ersten Entschließung zum Kommissionsvorschlag für „Ein hohes Datenschutzniveau für ganz Europa“ eingesetzt (siehe dazu Ziffer 18.3 dieses Berichts) und zum Verordnungsentwurf ausführlich Stellung genommen (Siehe hierzu https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/EU-Datenschutz_DSK/EU-Daten

schutzreform__Datenschutzkonferenz_nimmt_Stellung_zu_den_Entw__rfen.php). In der Anhörung des Innenausschusses des Deutschen Bundestages erhielt ich die Gelegenheit, dafür zu plädieren, mit Hilfe einer entsprechend veränderten Datenschutz-Grundverordnung ein hohes Mindestdatenschutzniveau in Europa zu erreichen (Videoaufzeichnung und Dokumente finden Sie unter dem Link http://www.bundestag.de/dokumente/textarchiv/2012/40998184_kw43_pa_inneres/index.html).

Die europaweite Diskussion über den Kommissionsvorschlag hat deutlich gemacht, dass unsere Versuche, als „Datenschutzlobby" auf eine Veränderung des Entwurfes in Richtung auf ein hohes europäisches Mindestdatenschutzniveau hinzuwirken, nicht unwidersprochen bleiben. Auch diejenigen, die an einem kostengünstigen niedrigen Höchstdatenschutzniveau interessiert sind, artikulieren sich an vielen Stellen. So ist es dem Bundesministerium des Innern gelungen, gelegentlichen Zuspruch für den Gedanken zu bekommen, dass nicht alle personenbezogenen Daten relevant genug sind, um grundrechtlich geschützt zu werden. Dieser Auffassung, die mit der Erkenntnis des Bundesverfassungsgerichtes kollidiert, wonach es kein belangloses Datum gibt, ist die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit ihrer Entschließung „Europäische Datenschutzreform konstruktiv und zügig voranbringen!" entschieden entgegengetreten (siehe dazu Ziffer 18.9 dieses Berichts). Gerade im Zeitalter von immer detaillierteren Persönlichkeitsprofilen, die auf einer Vielzahl von einzeln gesehenen scheinbar belanglosen Daten beruht, verbietet sich ein solcher Ansatz.

Im Folgenden sollen die aus datenschutzrechtlicher Sicht an den Verordnungsvorschlag zu richtenden Forderungen in Auszügen dargestellt werden.

### 1.2.1 Hohes Mindestdatenschutzniveau statt Vollharmonisierung

Dass der Kommissionsentwurf das Schutzziel des freien Datenverkehrs dem Schutzziel Datenschutz vorzieht, zeigt sich am stärksten im Postulat der Vollharmonisierung. Mit der Wahl der Rechtsform Verordnung bei gleichzeitigem Verzicht auf Öffnungsklauseln für nationalstaatliches Recht, das den Datenschutz stärker gewährleisten kann, setzt sich die Kommission dafür ein, dass in allen Mitgliedsstaaten identische Regelungen gelten und in exakt identischer Weise durchgesetzt werden. Der Eindruck, dass der Kommissionsentwurf damit die beiden Ziele Datenschutz und freien Datenverkehr gleichermaßen in den Blick nimmt, täuscht.

Dass die Vollharmonisierung der Erleichterung des freien Datenverkehrs dient, ist einleuchtend: Wenn überall in der Europäischen Union (EU) identische Regelungen gelten und durchgesetzt werden, können die Daten fließen ohne an den Grenzen aufgehalten zu werden.

Eine Vollharmonisierung dient demgegenüber gerade nicht in jedem Fall dem Recht der natürlichen Personen auf Schutz ihrer personenbezogenen Daten. Für das Schutzziel Datenschutz hängt die Wirkung einer Vollharmonisierung vielmehr allein vom dadurch gewährten Datenschutzniveau ab. Vollharmonisierung bedeutet nur dann einen Vorteil, wenn die europaweit identischen Regelungen für den Datenschutz Verbesserungen bedeuten. Für das Schutzziel des Datenschutzes kann eine Vollharmonisierung sogar nachteilig sein. Das wäre dann der Fall, wenn die vollharmonisierten Regelungen den Datenschutz weniger gewährleisteten, als es zuvor der Fall war. Die Aussage im Kommissionsentwurf, ein hohes Maß an Datenschutz für die Einzelnen sei gewährleistet, wenn der Schutz der Rechte und Freiheiten von Personen bei der Verarbeitung dieser Daten in allen Mitgliedsstaaten gleichwertig sei, wenn also europaweit die gleichen Regelungen gelten, ist vor allem dann falsch, wenn das Schutzziel nicht nur ein irgendwie hohes (oder niedriges) Maß an Datenschutz sondern ein höchstmögliches Maß an Datenschutz ist. Das muss es aus Datenschutzsicht aber sein. Für den Grad der Verwirklichung des Rechtes auf Datenschutz ist also allein die Höhe des Schutzniveaus entscheidend. Ob dieses Niveau in allen Mitgliedsstaaten exakt gleich hoch ist, ist für das Schutzziel Datenschutz dann unerheblich, wenn in allen Mitgliedsstaaten ein höchstmögliches Datenschutzniveau zur Pflicht gemacht wird, das nur überschritten, aber nicht unterschritten werden darf.

Das Postulat der Vollharmonisierung steht damit für den Vorrang der Erleichterung des freien Datenverkehrs vor dem Schutz der personenbezogenen Daten der Menschen in Europa. Aus Sicht des Datenschutzes muss der Kommissionsvorschlag

daher in die Richtung verändert werden, dass an die Stelle der Vollharmonisierung die Gewährleistung eines möglichst hohen Schutzniveaus für den Datenschutz tritt.

Dem Gegenargument, eine solche Regelung würde den freien Datenverkehr behindern, kann durch den Hinweis darauf begegnet werden, dass die EU für die Bereiche Verbraucherschutz und Umweltschutz, die ebenfalls geeignet sind, den freien Datenverkehr beziehungsweise Warenverkehr zu beschränken, Öffnungsklauseln kennt. In diesen Bereichen können die Mitgliedsstaaten nationales Recht schaffen, das die Ziele Verbraucherschutz und Umweltschutz stärker schützt, als es die europarechtlichen Regelungen tun. Die europäische Wirtschaft erscheint im Bereich des Datenschutzes nicht schutzwürdiger als im Bereich des Umweltschutzes und Verbraucherschutzes. Zudem gibt es einen großen Überschneidungsbereich zwischen datenschutzrechtlichen und verbraucherschutzrechtlichen Regelungen.

Die Forderung nach einem hohen Mindestdatenschutzniveau kann sich noch auf weitere Gründe stützen:

Erklärtes Ziel des Kommissionsvorschlages für die Datenschutz-Grundverordnung ist es, bei den Menschen in Europa Vertrauen in die Sicherheit ihrer personenbezogenen Daten im Internet zu schaffen. Alle Anstrengungen in diese Richtung müssen beachten, dass Vertrauen nur dort entsteht, wo es berechtigt ist. Wenn die Datenschutz-Grundverordnung nur ein Etikettenschwindel ist, dann wird bei den Menschen in Europa das Vertrauen in die Sicherheit ihrer Daten im Internet zu Recht nicht entstehen. Deshalb muss das europäische Datenschutzniveau so hoch wie möglich sein, es muss so hoch sein, dass die personenbezogenen Daten wirklich sicher sind. Solange es der Verordnung nur wichtig ist, dass in Europa überall dieselben Regelungen gelten und es nicht im Vordergrund steht, wie viel Datenschutz diese Regelungen bewirken können, kann das Vertrauen der Menschen in Europa nicht entstehen.

Und dieses das Vertrauen begründende hohe Datenschutzniveau sollte nicht statisch festgeschrieben werden, ohne den Mitgliedsstaaten innovative Regelungen zu erlauben, die auf technische Entwicklungen reagieren und den Datenschutz noch besser gewährleisten. Die Entwicklung von kreativen neuen Lösungen für besseren Datenschutz darf in Europa nicht durch die Formulierung von starren Höchststandards behindert werden. Heterogene Gruppen sind kreativer als homogene Gruppen. Im Föderalismus zeigt sich, dass viele unterschiedliche Einheiten viele unterschiedliche Problemlösungen finden. Eine Rechtsfortbildung zur Stärkung des Datenschutzniveaus würde also erleichtert, wenn in der Verordnung Mindeststandards formuliert würden, über die alle Mitgliedsstaaten hinausgehen, die aber nicht unterboten werden dürfen.

### 1.2.2 Reduzierung der Befugnisse der Kommission zur Rechtsetzung

Im Kommissionsvorschlag findet sich eine überwältigende Vielzahl von Ermächtigungen zum Erlass von delegierten Rechtsakten, also von Rechtsakten, die die Kommission selbst unter geringerer Beteiligung des Europäischen Parlamentes und des Rates erlässt. Angesichts der oben beschriebenen Präferenz der Kommission für das Schutzziel des freien Datenverkehrs vor dem Schutzziel des Datenschutzes sollte darauf verzichtet werden, der Kommission diese umfassende Möglichkeit zur Setzung von bindendem Recht für alle Mitgliedsstaaten zu geben.

Stattdessen sollten entsprechende Regelungen in der Verordnung selbst oder in anderen europäischen Rechtsakten mit Gesetzescharakter, also in Verordnungen oder Richtlinien geregelt werden. Sofern diese Forderung nicht durchsetzbar ist, sollte gleichwohl auf Ermächtigungen für delegierte Rechtsakte verzichtet werden. Dies hätte zur Folge, dass – sofern der hier erhobenen Forderung nach dem Verständnis der Verordnung als Normierung von Mindeststandards gefolgt wird – an ihre Stelle Normen träten, die durch mitgliedsstaatliche Parlamente verabschiedet würden, die ihrerseits an die durch die Verordnung statuierten Mindeststandards gebunden wären. Sofern der Forderung nach Mindeststandards nicht gefolgt würde, träte an die Stelle der delegierten Rechtsakte die Auslegung der Verordnung durch die datenschutzrechtlichen Kontrollbehörden und Rechtsprechung, die aufgrund dieser Entscheidungen ergangen ist.

Für entgegen dieser Forderung verbleibende Ermächtigungen zu delegierten Rechtsakten muss ein weiterer Punkt beachtet werden: Bei den in Artikel 86 des Kommissionsvorschlages genannten Ermächtigungen zu delegierten Rechtsakten

sind zwei unterschiedliche Arten zu unterscheiden. Bei einem ersten Teil können Europäisches Parlament oder Rat die Ermächtigung zum Erlass der delegierten Rechtsakte widerrufen. Dies gilt für die in Artikel 86 Absatz 3 des Kommissionsvorschlages genannten Regelungsgegenstände. Bei einem zweiten Teil ist Wirksamkeitsvoraussetzung der delegierten Rechtsakte, dass weder Europäisches Parlament noch Rat Einwände gegen den delegierten Rechtsakt erheben. Dies gilt für die in Absatz 5 genannten Regelungsgegenstände. Angesichts der oben beschriebenen Neigung der Kommission, den freien Datenverkehr vor dem Datenschutz zu privilegieren, muss aus Datenschutzsicht gefordert werden, dass die Beteiligung des Europäischen Parlamentes so stark wie möglich ist. Daher sollten die nach einer sehr kritischen Prüfung verbleibenden Ermächtigungen der Kommission zu delegierten Rechtsakten auf jeden Fall daran gebunden werden, dass Europäisches Parlament oder Rat keine Einwände erhoben haben.

### 1.2.3 Reduzierung der weitreichenden Befugnisse der Kommission zur Rechtsdurchsetzung

Auch die im Kommissionsvorschlag vorgesehenen Regelungen über die Aufsichtsbehörden, also zum Vollzug und zur Rechtsdurchsetzung, sind Regelungen, die dem Ziel der Vollharmonisierung dienen. Diesen Vorschlägen müssen Forderungen nach dem Verzicht auf Regelungen, nach denen die Kommission Rechte der Rechtsdurchsetzung erlangt, und nach der alleinigen Verpflichtung der unabhängigen Aufsichtsbehörden auf den Datenschutz gegenübergestellt werden.

Der europäische Datenschutzausschuss soll nach dem Kommissionsvorschlag von den Leiterinnen und Leitern der datenschutzrechtlichen Aufsichtsbehörden aller Mitgliedsstaaten und dem oder der europäischen Datenschutzbeauftragten gebildet werden. Er soll gegenüber der Kommission umfassende Informationspflichten haben. Auch soll die Kommission Maßnahmen der unabhängigen nationalen Aufsichtsbehörden bis zu zwölf Wochen aussetzen können, beispielsweise um in der Zwischenzeit einen Durchführungsrechtsakt in der Form eines „Beschlusses über die ordnungsgemäße Anwendung der Verordnung“ zu erlassen. Hierbei ist besonders beachtlich, dass – sofern die Maßnahme der unabhängigen Aufsichtsbehörde der Verhinderung eines Datenschutzverstoßes dient – in der Zwischenzeit schwerwiegende Verletzungen des Rechtes auf Schutz der personenbezogenen Daten geschehen können. Auch der im Kommissionsvorschlag vorgesehene Erlass von „sofort geltenden Durchführungsrechtsakten“ in „hinreichend begründeten Fällen äußerster Dringlichkeit“ stellt einen tiefen Eingriff in die Unabhängigkeit der Aufsichtsbehörden dar. Mit Hilfe des „Kohärenzverfahrens“ soll die europaweite Einheitlichkeit der aufsichtsbehördlichen Einzelentscheidungen hergestellt werden. Sofern die für die Verordnung vorgeschlagenen Regelungen nicht als Mindeststandards angesehen würden, käme das Kohärenzverfahren allein dem freien Datenverkehr zugute, weil es allein auf die Einheitlichkeit, nicht auf ein möglichst hohes Datenschutzniveau zielt.

Dieser starken Rolle der Kommission quasi als Kontrollbehörde über die unabhängigen Aufsichtsbehörden steht die Auffassung des Europäischen Gerichtshofes zur Unabhängigkeit der datenschutzrechtlichen Kontrollstellen entgegen. Nach dem Europäischen Gerichtshof dürfen die Kontrollstellen bei der Wahrnehmung ihrer Aufgaben keinerlei Weisungen unterliegen. Sie müssen „von jeglicher Einflussnahme von außen einschließlich der unmittelbaren oder mittelbaren Einflussnahme des Bundes oder der Länder sicher sein“. Hiervon muss auch die Freiheit vor Einflussnahmen der EU-Kommission umfasst sein.

Aber selbst dann, wenn sich die Kommission selbst als unabhängige oberste Aufsichtsbehörde sähe, die ihre starke Rolle gegenüber den unabhängigen Aufsichtsbehörden der eigenen Unabhängigkeit und der Eigenschaft als „Hüterin der Verträge“ verdankt, würde dies in krassem Widerspruch zur Auffassung des Europäischen Gerichtshofes stehen. In seinem Urteil vom 9. März 2010 zeigt der Europäische Gerichtshof durch die Wahl der Szenarien für mögliche Beeinträchtigungen der Unabhängigkeit der datenschutzrechtlichen Kontrollstellen, dass auch er strukturell eher den Datenschutz als den freien Datenverkehr als das schutzbedürftigere Schutzgut ansieht. So bildet er Beispiele dafür, dass mitgliedsstaatliche Regierungen möglicherweise ein Interesse an der Nichteinhaltung der Datenschutzvorschriften hätten, weil sie – etwa im Fall einer Kooperation von öffentlichen und privaten Stellen oder im Rahmen öffentlicher Aufträge an private Stellen – selbst involvierte Partei dieser Bearbeitung sein könnten oder ein besonderes Interesse am Zugang

zu Datenbanken haben könnten. An dieser Stelle der Urteilsbegründung heißt es weiter: „Im Übrigen könnte diese Regierung auch geneigt sein, wirtschaftlichen Interessen den Vorrang zu geben, wenn es um die Anwendung der genannten Vorschriften durch bestimmte Unternehmen geht, die für das Land oder die Region wirtschaftlich von Bedeutung sind". Warum die Kommission glaubt, diese strukturellen Bedrohungen der Unabhängigkeit gälten nicht für sie selbst, ist schwer erklärlich. Dies gilt insbesondere nach der Lektüre der folgenden Urteilspassage, in der der Europäischer Gerichtshof begründet, warum „bereits die bloße Gefahr einer politischen Einflussnahme der Aufsichtsbehörden auf die Entscheidungen der Kontrollstellen ausreicht, um deren unabhängige Wahrnehmung ihrer Aufgaben zu beeinträchtigen". Es könne nämlich – wie die Kommission selbst vorgetragen hat – einen „vorauseilenden Gehorsam" der Kontrollstellen geben. Auch fordere ihre Rolle als „Hüter des Rechts auf Privatsphäre, dass ihre Entscheidungen, also sie selbst, über jeglichen Verdacht der Parteilichkeit erhaben" sei. All diese Argumente sprechen dagegen, der Kommission als derjenigen Institution der Europäischen Union, die vor allem eine exekutive Funktion hat, relevante Befugnisse gegenüber den unabhängigen Aufsichtsbehörden zu geben.

Nach der jetzt geltenden Datenschutz-Richtlinie 95/46 kommt den „unabhängigen Kontrollstellen" die Aufgabe der Überwachung der Anwendung der von den Mitgliedsstaaten zur Umsetzung der Richtlinie erlassenen Vorschriften zu. Dabei stehen die Schutzziele freier Datenverkehr und Datenschutz nach der Richtlinie in einem Verhältnis, das zugleich der Binnenmarktlogik und dem Schutz der Privatsphäre verpflichtet ist: Weil Datenschutz Kosten verursacht, wurde die Wirtschaft in Ländern mit einem höheren Datenschutzniveau vor Erlass der Richtlinie im Verhältnis zur Wirtschaft in Ländern mit einem niedrigeren Datenschutzniveau benachteiligt. Daher musste das Datenschutzniveau in Ländern mit einem niedrigeren Datenschutzniveau angehoben werden. Dabei wird dem Postulat gefolgt, wonach die Angleichung der Rechtsvorschriften in den Mitgliedsstaaten nicht zu einer Verringerung des Schutzes für das Recht auf die Privatsphäre führen darf. Genau dieser Logik sind die unabhängigen Kontrollstellen nach Artikel 28 Absatz 1 der Datenschutz-Richtlinie 95/46 verpflichtet. Bei der Anwendung der angeglichenen Rechtsvorschriften zur Erleichterung des Binnenmarktes stehen sie dafür, dass keine Absenkung des Schutzniveaus für den Datenschutz erfolgt, sondern „im Gegenteil (. . .) in der Gemeinschaft ein hohes Schutzniveau" sichergestellt ist. Insofern ist die Einrichtung unabhängiger Kontrollstellen „ein wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogener Daten" gewesen. Auch der Europäische Gerichtshof spricht von der „Rolle der Kontrollstellen als Hüter des Rechts auf Privatsphäre". Nur mit dieser Ausrichtung darauf, dass bei der Erleichterung des Binnenmarktes keine Absenkung des Datenschutzniveaus erfolgt, sind die Datenschutzbehörden also nach der gegenwärtig geltenden Datenschutz-Richtlinie 95/46 auch dem Schutz der Freiheit des Datenverkehrs verpflichtet.

Nach dem Verordnungsvorschlag der Kommission sollen die Aufgaben der unabhängigen Datenschutzbehörden künftig auf ein anderes Ziel ausgerichtet sein: Sie sollen einen Beitrag zur einheitlichen Anwendung der scheinbar den beiden Schutzzielen Datenschutz und freier Datenverkehr gleichermaßen verpflichteten, in Wirklichkeit aber den freien Datenverkehr privilegierenden Verordnung leisten, „damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung ihrer Daten geschützt und der freie Datenverkehr in der Union erleichtert werden".

Angesichts der zwischenzeitlichen Verankerung des Rechtes auf Datenschutz in der Grundrechtecharta hätte es nahe gelegen, ganz darauf zu verzichten, die unabhängigen „Datenschutzbehörden" explizit auch auf das Schutzziel des freien Datenverkehrs zu verpflichten. Dies scheint angesichts der Privilegierung des freien Datenverkehrs durch den Kommissionsvorschlag sogar geboten.

### 1.2.4 Regelung verbindlicher technischer Anforderungen in der Verordnung selbst

Im Verordnungstext selbst müssen sich – anders als dies im Kommissionsvorschlag der Fall ist – Regelungen finden, die für die IT-Sicherheit (IT = Informationstechnik) und den technischen und organisatorischen Datenschutz erforderlich sind. Dass dies im Kommissionsvorschlag nicht der Fall ist, sondern die für die IT-Sicherheit und den technikbezogenen und organisationsbezogenen Datenschutz erforderlichen Regelungen dem Erlass direkter Rechtsakte vorbehalten bleiben sollen, ist Ausdruck des Vorranges des Schutzzieles freier Datenverkehr vor dem Schutzziel Datenschutz.

Es ist deshalb problematisch, weil die überwiegende Vielzahl datenschutzrechtlicher Probleme gar nicht erst entstehen würde, wenn datenschutzgerechtere technische und organisatorische Maßnahmen ergriffen würden. Da IT-Produkte gegenwärtig in der Regel so erstellt werden, dass viele für den beabsichtigten Zweck nicht erforderliche Daten entstehen, erscheint das Ergreifen von technischen und organisatorischen Maßnahmen, die auf diese nicht erforderlichen Datenmengen reagieren, als kostenintensiv. Diese Situation sollte schon im Vorhinein vermieden werden. Insbesondere

— sollte die Bedeutung des technischen und organisatorischen Datenschutzes betont werden. Es sollte daher ausdrücklich als Grundsatz normiert werden, dass personenbezogene Daten unter Beachtung der erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz verarbeitet werden müssen,

— sollte die Erforderlichkeit von technischen und organisatorischen Maßnahmen zum Datenschutz allein an der Tiefe des Eingriffs in das Datenschutzrecht und nicht an der Höhe der Implementierungskosten gemessen werden,

— sollten die elementaren Datenschutzziele Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit als grundsätzliche Zielvorgaben aller technischen und organisatorischen Maßnahmen normiert werden,

— sollte klargestellt werden, dass Datenschutz durch Technik auch die Auswahl und Gestaltung von Datenverarbeitungssystemen betrifft,

— sollten den Verantwortlichen Risikoanalysen, Risikobewertungen und Sicherheitskonzepte zur Pflicht gemacht werden,

— sollten die Verantwortlichen nach dem Stand der Technik zur weitestmöglichen Anonymisierung und Pseudonymisierung verpflichtet werden,

— sollte für das Internet ein Recht auf Nutzung von Pseudonymen statuiert werden,

— sollten die Verpflichtungen normiert werden, Geräte und Programme datensparsam und datenschutzgerecht herzustellen (privacy by design) und Grundeinstellungen von Geräten und Programmen datensparsam und datenschutzgerecht vorzunehmen (privacy by default),

— sollte ausdrücklich klargestellt werden, dass die Regelungen der Verordnung auch für das Tracking im Internet gelten,

— sollte auf die spezifischen Probleme schon jetzt eingesetzter Techniken wie Videoüberwachung und Chipkarten reagiert werden.

#### 1.2.5 Verzicht auf Angemessenheitsbeschluss, jedenfalls Bindung an schärfere Voraussetzungen

Die Kommission gibt sich im Verordnungsvorschlag selbst die Befugnis, Nicht-EU-Länder als datenschutzrechtlich unbedenklich zu erklären. Bei dieser Entscheidung muss sie elementare Anforderungen wie Rechtsstaatlichkeit nur berücksichtigen. Auf das Instrument dieses „Angemessenheitsbeschlusses“ sollte verzichtet werden. Auch er bewirkt einen Vorrang des freien Datenverkehrs vor dem Datenschutz, weil Folge eines solchen Beschlusses ist, dass Datenübermittlungen in Drittländer ohne weitere Voraussetzung vorgenommen werden dürfen, selbst wenn diese im Einzelfall das Recht auf Datenschutz beschränken.

Beispielsweise die gegenwärtigen datenschutzrechtlichen Debatten der nationalen Datenschutzbehörden mit Unternehmen mit Sitz in den Vereinigten Staaten von Amerika (USA) zeigen, dass die Forderung nach der Beachtung angemessener datenschutzrechtlicher Standards durch Unternehmen aus den USA konterkariert würde, wenn die Kommission die USA in dieser Weise pauschal frei zeichnen würde. Diese Regelung sollte gestrichen werden.

Hilfsweise sollte die Entscheidung der Kommission an strengere Voraussetzungen gebunden werden, als dies nach dem Kommissionsvorschlag der Fall ist. Es reicht nicht, dass die Rechtsstaatlichkeit, „die Existenz wirksamer und durchsetzbarer Rechte einschließlich wirksamer administrativer und gerichtlicher Rechtsbehelfe für betroffene Personen, insbesondere für in der Europäischen Union ansässige betroffene Personen, deren personenbezogene Daten übermittelt werden“ und an-

dere Kriterien lediglich „bei der Prüfung der Angemessenheit des gebotenen Schutzes“ von der Kommission „berücksichtigt“ werden. Stattdessen müsste die Erfüllung der genannten Voraussetzungen zur Voraussetzung für einen Angemessenheitsbeschluss gemacht werden.

### 1.2.6 Keine Privilegierung von kleinsten, kleinen und mittleren Unternehmen

Ein weiterer Ausdruck des Vorranges für das Schutzziel des freien Datenverkehrs vor dem Schutzziel des Datenschutzes sind die im Verordnungsvorschlag vorgesehenen Regelungen zur Privilegierung von kleinsten, kleinen und mittleren Unternehmen, die eine Abwägung des Zieles der Schaffung von Erleichterungen für kleinste, kleine und mittlere Unternehmen mit dem Ziel des Datenschutzes vermissen lassen. So ist nicht auf die Größe des datenschutzrechtlich verantwortlichen Unternehmens abzustellen, sondern auf die Tiefe des Eingriffes in das Datenschutzrecht.

Die Regelung, wonach bei der Verarbeitung personenbezogener Daten eines Kindes „spezifische Maßnahmen für Kleinstunternehmen und Kleinunternehmen sowie mittlere Unternehmen“ geregelt werden können, ist zu streichen. Für den Grad der Betroffenheit des Datenschutzrechtes von Kindern spielt es keine Rolle, ob ihre personenbezogenen Daten durch Kleinstunternehmen, Kleinunternehmen, mittlere Unternehmen oder größere Unternehmen verarbeitet werden. Es kommt vielmehr auf die Tiefe des Eingriffes an. Die vorgesehenen Ausnahmen für die Datenverarbeitung durch Kleinstunternehmen, Kleinunternehmen und mittlere Unternehmen bei Verfahren und Vorkehrungen, damit die betroffene Person ihre Rechte ausüben kann, bei der Information der betroffenen Personen und bei den Pflichten des für die Verarbeitung Verantwortlichen sind zu streichen, weil die Ausnahmen nicht auf die Tiefe des Eingriffs für die Betroffenen abstellen. So ist es auch nicht einleuchtend, warum bei den Regelungen zur Verpflichtung zur Benennung einer oder eines betrieblichen Datenschutzbeauftragen und zur Verpflichtung für Datenverarbeiter mit Sitz außerhalb der Europäischen Union zur Bestellung einer Vertreterin oder eines Vertreters darauf abgestellt wird, dass das betreffende Unternehmen mehr als 250 Mitarbeiterinnen und Mitarbeiter beschäftigt, ohne darauf zu achten, ob von diesen Beschäftigten risikobehaftete Datenverarbeitungen vorgenommen werden oder nicht.

### 1.2.7 Änderungserfordernisse bei den Regelungen zu Einwilligungen

Bei der Beschreibung der Wirksamkeitsvoraussetzungen für Einwilligungen in Artikel 7 des Kommissionsentwurfes fehlt die Informiertheit der Entscheidung. Dies ist auch nach der selbstgesetzten Logik des Kommissionsvorschlages unbedingt zu korrigieren, weil die Transparenz der Datenverarbeitung eine wesentliche Voraussetzung für das Vertrauen der Betroffenen ist. Sie müssen nicht nur genau wissen, was die Zwecke der Datenverarbeitung sind, sondern auch, welche Daten genau erhoben werden, woher sie gegebenenfalls stammen, was genau mit ihnen geschehen wird, wer der für die Datenverarbeitung Verantwortliche ist und wann die Daten gelöscht werden. Weiterhin ist klarzustellen, dass sich Einwilligungen nicht auf technisch-organisatorische Maßnahmen erstrecken. Auch bei der Profilbildung und beim Direktmarketing sollten Einwilligungen gefordert werden. Beim Direktmarketing war dies im Vorentwurf des Kommissionsvorschlages der Fall. Die Streichung ist vermutlich auf erfolgreiche Lobbyarbeit der interessierten Verbände zurückzuführen.

### 1.2.8 Verantwortlichkeit auch für Inhalte

In der Definition des für die Verarbeitung Verantwortlichen des Kommissionsentwurfes heißt es, es handele sich um Stellen, die allein oder gemeinsam mit anderen „über die Zwecke, Bedingungen und Mittel der Verarbeitung von personenbezogenen Daten“ entscheiden. Hierbei fehlt die Verantwortlichkeit für Inhalte, obwohl der Personenbezug von Daten ja entscheidend durch deren Inhalt geprägt ist und der Berichtigungsanspruch gegenüber dem Verantwortlichen besteht.

## 1.3 facebook, microsoft & Co. frohlocken und fechten für ein niedriges Datenschutzniveau in Europa

Und nun schließt sich der Kreis: Wie stehen die großen, in den Vereinigten Staaten von Amerika ansässigen Unternehmen, die massenhaft Daten der Menschen in der Europäischen Union (EU) verarbeiten, zum Kommissionsentwurf?

Einerseits frohlocken facebook, microsoft & Co. Erfüllt doch der Vorschlag der EU-Kommission im Wesentlichen ihren langgehegten und häufig geäußerten Wunsch danach, sich nicht jeweils auf Aufsichtbehörden in Kiel, Hamburg, Irland, Österreich, Frankreich, Schweden und Bremen einstellen zu müssen. Anlässlich einer Veranstaltung des EU-Parlamentes am 9. und 10. Oktober 2012 in Brüssel freute sich der sympathische französischsprachige Vertreter von microsoft darüber und rief mehrfach vom Podium „c´est fantastique!" („Das ist fantastisch!"). Seine Freude ist verständlich: Die Vertreterinnen und Vertreter des freien Datenverkehrs haben sich vollständig durchgesetzt und können sich jetzt darauf konzentrieren, ihre argumentativen Ressourcen für die Senkung des im Kommissionsvorschlag normierten Datenschutzes einzusetzen.

Dass und wie die wirtschaftlichen Interessengruppen für eine Senkung des europäischen Datenschutzniveaus fechten, zeigt ein von der Initiative „europe-vs-facebook" veröffentlichtes „Lobby-Dokument". Hierin findet sich die Stellungnahme facebooks zum Kommissionsvorschlag für die Datenschutz-Grundverordnung. Das Dokument ist verfasst worden, um der irischen Regierung zu „helfen, ihren Beitrag zu der Debatte auf EU-Ebene zu leisten".

In einem einzigen Punkt deckt sich facebooks Stellungnahme mit der hier vertretenen Auffassung. Allerdings ist die Motivation genau die entgegengesetzte: Auch facebook fürchtet delegierte Rechtsakte der Kommission. Allerdings resultiert facebooks Befürchtung vermutlich aus einer Angst vor strengen Datenschutzregelungen, wohingegen von Datenschutzseite Regelungen befürchtet werden, die den Datenschutz zugunsten des freien Datenverkehrs aus dem Blick verlieren.

In allen anderen Punkten vertritt facebook die gegenteilige Auffassung zu den von Datenschützerinnen und Datenschützern formulierten Forderungen:

— Facebook wendet sich gegen europaweit verbindliche technische Regelungen, die „frustrierend und kostspielig" seien. Stattdessen sollten best practices „von Firmen wie facebook" ermutigt werden.

— Facebook „heißt" das im Kommissionsvorschlag enthaltene Prinzip der alleinigen Zuständigkeit einer Datenschutzaufsichtsbehörde „willkommen", fürchtet aber, es könne unterlaufen werden. Für Daten, die die in den Vereinigten Staaten von Amerika sitzende facebook Inc. verarbeite, „dränge" facebook die Entscheiderinnen und Entscheider, klarzustellen, dass nur diejenige Aufsichtsbehörde zuständig sei, in deren Land bereits ein zu der Unternehmensgruppe gehörender Verantwortlicher ansässig sei. Auch müsse verhindert werden, dass andere europäische Datenschutzbehörden vorläufige Maßnahmen treffen könnten, wenn die zuständige Aufsichtsbehörde nicht innerhalb eines Monats auf eine Anfrage der anderen Behörde antwortet. Die Möglichkeit gemeinsamer Aktionen von Aufsichtsbehörden sei abzulehnen. Auch werde die Macht der zuständigen Behörde durch den Kohärenzmechanismus unterminiert, in den der neu einzurichtende europäische Datenschutzausschuss, die Kommission und andere Aufsichtsbehörden einbezogen seien. Dieser Mechanismus könne bedeutende Auswirkungen auf die Innovationszyklen haben.

— Das Prinzip „privacy bei default", also die Verpflichtung, datenschutzgerechte Voreinstellung vorzunehmen, berücksichtige den „Ethos des Teilens" nur ungenügend und werde daher abgelehnt.

— Facebook hält es für unangemessen, dass der Kommissionsvorschlag alle Menschen unter 18 Jahren dem Minderjährigenschutz unterstellt und schlägt vor, die Altersgrenze auf 13 festzulegen, wie es facebook nach seinen Nutzungsbedingungen mache.

— Einwilligungsregelungen sollten nicht zu einem „zerrissenen" Internet führen. Die jetzt vorgesehenen Regelungen würden zu einer Überflutung der Nutzerinnen und Nutzern mit Einwilligungsfragen bedeuten. Das Unternehmen facebook macht sich hier Sorgen, dass dies zu einer Entwertung des Prinzips der Einwilligung führen würde.

— Facebook sorgt sich wegen der zu stark reglementierenden Natur der im Kommissonsvorschlag vorgesehenen Sicherheitsvorschriften und der Tatsache, dass Datenpannen der zuständigen Aufsichtsbehörde binnen 24 Stunden angezeigt werden müssen. Dies binde zu sehr die Ressourcen der Aufsichtsbehörden. Auch könne facebook durch diese Regelungen gezwungen sein, alle Nutzerin-

nen und Nutzer zu informieren, die eine Seite, eine Gruppe oder ein Profil besucht hätten.

— Facebook fürchtet, dass die hohen Strafen für Datenschutzverstöße (es war der Wirtschaftslobby vor Veröffentlichung des Kommissionsvorschlages gelungen, die Höchstsumme von 5 % auf 2 % des globalen Ertrages von Wirtschaftsunternehmen zu reduzieren) die Investitionsanreize von Internetunternehmen in der Europäischen Union (EU) untergraben, was der EU einen großen Schlag versetzen würde, sei doch der Internetsektor der Hauptantrieb für die Schaffung von Arbeitsplätzen und Wachstum in einer „ansonsten todgeweihten wirtschaftlichen Umgebung". Die vorgeschlagenen Sanktionsregelungen würden bei den Staaten zu hohen Gerichtskosten führen.

Uns Datenschützerinnen und Datenschützern ist bewusst, dass wir in der Diskussion um den Datenschutz in Europa nicht zuletzt mit facebook & Co. ressourcenmächtige Gegner haben, die sich nicht scheuen, ihr wirtschaftliches Drohpotenzial zu nutzen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, in der Bremen am 1. Januar 2013 turnusmäßig den Vorsitz übernommen hat, wird sich dessen ungeachtet auch im Jahr 2013 für ein hohes Mindestdatenschutzniveau für die Menschen in Europa einsetzen.

Dr. Imke Sommer

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
der Freien Hansestadt Bremen

## 2. Bremische Bürgerschaft – Ergebnisse der Beratungen des 34. Jahresberichts

Der Bericht und Antrag des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zum 34. Jahresbericht der Landesbeauftragten für Datenschutz vom 16. März 2012 (Drucksache 18/302) und zur Stellungnahme des Senats vom 28. August 2012 (Drucksache 18/551) lag zum Redaktionsschluss noch nicht vor.

## 3. Behördliche und betriebliche Beauftragte für den Datenschutz

### 3.1 Workshops der behördlichen Datenschutzbeauftragten

Die Reihe der Workshops mit den behördlichen Datenschutzbeauftragten wurde auch im Berichtsjahr fortgesetzt. In Bremen fanden zwei Workshops und in Bremerhaven ein Workshop statt, die aufgrund des Interesses an den Themen der Workshops teilweise auch wiederholt wurden.

Thema des ersten Workshops in Bremen im vergangenen Jahr war „Fernwartung durch Dritte – welche Anforderungen sind zu erfüllen?“. Fernwartung durch Dritte, das heißt durch externe Stellen, zum Beispiel eine Softwarewartung durch die Herstellerfirma oder Outsourcing des User-Helpdesks, ist, sofern sie von Dritten für Stellen durchgeführt wird, bei denen das Bremische Datenschutzgesetz (BremDSG) zur Anwendung gelangt, rechtlich als Datenverarbeitung im Auftrag nach § 9 BremDSG zu bewerten. Bei der Verarbeitung personenbezogener Daten im Auftrag verbleibt die Verantwortung für die Verarbeitung bei der auftraggebenden Stelle. Die Vergabe und die Durchführung des Fernwartungsauftrags sind nur unter Einhaltung der in § 9 BremDSG enthaltenen Anforderungen zulässig. Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftraggeber hat sich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen beim Auftragnehmer zu überzeugen. Die zu ergreifenden technischen und organisatorischen Maßnahmen finden ihre Grundlage speziell in § 7 BremDSG. In der bremischen Verwaltung werden Fernwartungsaktivitäten in zunehmendem Maße von der Anstalt öffentlichen Rechts Dataport wahrgenommen. Hieraus ergeben sich gerade auch für die Tätigkeit der behördlichen Datenschutzbeauftragten besondere Fragestellungen, die im Workshop mit den behördlichen Datenschutzbeauftragten näher erörtert wurden.

Der zweite Workshop befasste sich schwerpunktmäßig mit dem Thema „Kommissionsentwurf zur Datenschutz-Grundverordnung der Europäischen Union (EU)“. Mit der EU-Datenschutz-Grundverordnung möchte die EU-Kommission das Datenschutzrecht in Europa harmonisieren und für Europa einheitliche Datenschutzanforderungen erlassen. Die Verordnung soll an die Stelle der bisherigen EU-Datenschutzrichtlinie treten und alle in ihrem Geltungsbereich geltenden mitgliedsstaatlichen Regelungen verdrängen. Auch die Datenschutzgesetzgebung im Land Bremen und somit die Funktion der behördlichen Datenschutzbeauftragten wären von der Verordnung betroffen. Der Entwurf der Verordnung stößt bei den Datenschützerinnen und Datenschützern auf erhebliche Kritik, beträchtliche Veränderungen zur Verbesserung des Datenschutzniveaus werden von ihnen empfohlen. Die Teilnehmerinnen und Teilnehmer nahmen mit großem Interesse an dem Workshop teil.

In Bremerhaven befasste sich der Workshop schwerpunktmäßig mit dem Thema „facebook – Kommunikation unter Freunden?“ (siehe auch 34. Jahresbericht, Ziffer 3.1). Wie in Bremen bestand auch hier großes Interesse am Thema, es ergaben sich lebhafte Diskussionen.

In allen Workshops bestand darüber hinaus für die Teilnehmenden wieder die Möglichkeit, sich über die bei ihrer Tätigkeit gesammelten Erfahrungen auszutauschen. Die Workshops mit den behördlichen Datenschutzbeauftragten sollen im Jahr 2013 fortgesetzt werden.

### 3.2 Gesetzeskonforme Bestellung behördlicher Datenschutzbeauftragter

Die dem Bremischen Datenschutzgesetz (BremDSG) unterliegenden Stellen haben gemäß § 7 a BremDSG behördliche Datenschutzbeauftragte zu bestellen. Die Datenschutzbeauftragten sind bei Erfüllung ihrer Aufgaben weisungsfrei und dürfen deswegen nicht benachteiligt werden. Sie sind im erforderlichen Umfang freizustellen und bei der Erfüllung ihrer Aufgaben zu unterstützen. Die Bestellung kann

in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches (BGB) widerrufen werden. Die behördlichen Datenschutzbeauftragten wirken auf die Einhaltung dieser Gesetze und anderer Vorschriften über den Datenschutz hin.

Im Berichtsjahr waren wir wiederholt mit Fällen befasst, bei denen die betreffenden öffentlichen Stellen § 7 a BremDSG nicht nachgekommen sind, weil sie die Bestellung einer beziehungsweise eines behördlichen Datenschutzbeauftragten nicht vornahmen oder den sich aus dieser Bestimmung ergebenden Anforderungen nicht entsprachen. Wiederholt machten wir die genannten Stellen auf die Notwendigkeit der gesetzeskonformen Bestellung behördlicher Datenschutzbeauftragter aufmerksam. Auf die Unverzichtbarkeit der Datenschutzbeauftragten wiesen wir bereits in letzten Jahr hin (vergleiche 34. Jahresbericht, Ziffer 3.2).

Wir stellten fest, dass bei einer großen bremischen Behörde mit zahlreichen Verfahren personenbezogener Datenverarbeitung seit mehr als eineinhalb Jahren das Amt der beziehungsweise des behördlichen Datenschutzbeauftragten nicht wiederbesetzt wurde. Trotz mehrfacher Aufforderung kam die Behörde ihren Pflichten nach § 7 a BremDSG nicht nach. Die Bestellung mit der daran anschließenden Mitteilung an die Landesbeauftragte für Datenschutz und Informationsfreiheit hätte unverzüglich, spätestens einen Monat nach der Amtsniederlegung des bisherigen Funktionsinhabers, in Schriftform erfolgen müssen. Wiederholt kam die Behörde mündlichen Zusagen zur Bestellung einer beziehungsweise eines behördlichen Datenschutzbeauftragten und zur Erteilung einer Meldung nach § 7 a Absatz 5 BremDSG nicht nach. Die Nichtbestellung wurde von uns gegenüber dem zuständigen Senator nach § 29 BremDSG beanstandet. Der Senator begründete die Nichtbestellung einer beziehungsweise eines behördlichen Datenschutzbeauftragten mit dem in der betreffenden Behörde stattfindenden Reorganisationsprozess, der es nicht zulasse, für das Amt der oder des behördlichen Datenschutzbeauftragten personelle Ressourcen zur Verfügung zu stellen.

Als Zwischenlösung empfahl der Senator der Behörde, zunächst eine vertragliche Vereinbarung zur Aufgabenübertragung mit einem Datenschutzdienstleister abzuschließen und damit den Gesetzesauftrag zu erfüllen. Im weiteren Fortgang des Reorganisationsprozesses soll die Behörde dann bis Ende 2012 die Aufgabe der oder des behördlichen Datenschutzbeauftragten einer eigenen Mitarbeiterin oder eines eigenen Mitarbeiters übertragen. Die Umsetzung dieser Zielsetzung bleibt abzuwarten.

Auch in einem anderen Ressort wurden zur Umsetzung von § 7 a BremDSG Verträge mit einem Datenschutzdienstleister geschlossen. Gegenstand der Verträge ist die Erbringung von Datenschutzdienstleistungen. Die Verträge enthalten jeweils eine Regelung zur Bestellung des Geschäftsführers des Dienstleisters zum externen Datenschutzbeauftragten. Außerdem enthalten sie zahlreiche Regelungen, die auf unsere datenschutzrechtliche Kritik stoßen. So ist auch bei der Bestellung externer Datenschutzbeauftragter die Pflicht zur Wahrung von Berufsgeheimnissen oder Amtsgeheimnissen, in diesem Fall des Sozialgeheimnisses, zu beachten. Dieser Pflicht wurde mit den vertraglich vereinbarten Regelungen nicht entsprochen. Greift der externe Dienstleister zur Erfüllung seiner Aufgaben als behördlicher Datenschutzbeauftragter auf Sozialdaten zu, verlassen diese Daten den öffentlichen und gelangen in den nicht öffentlichen Bereich. Eine Befugnis zur Preisgabe der Sozialdaten gegenüber dem Dienstleister besteht nicht.

Aus § 7 a BremDSG ergibt sich, wie die Bestellung der behördlichen Datenschutzbeauftragten zu erfolgen hat und welche Aufgaben diese wahrzunehmen haben. Die Regelungen des § 7 a BremDSG können nicht durch vertragliche Vereinbarungen verdrängt werden. Der Umfang der sich aus dem Bremischen Datenschutzgesetz ergebenden Aufgaben darf vertraglich nicht beschränkt werden. Die Verträge enthalten darüber hinaus zahlreiche Regelungen, die mit den Aufgaben der behördlichen Datenschutzbeauftragten nicht zu vereinbaren sind. Nicht zu den Aufgaben der Datenschutzbeauftragten zählen unter anderem die Vorhaltung und Pflege des Verfahrensverzeichnisses, die Wahrung der Rechte Betroffener durch die Verfügbarmachung des Verzeichnisses und die Prüfung von Benachrichtigungspflichten, die Verpflichtung von Mitarbeiterinnen und Mitarbeitern auf das Datengeheimnis sowie die Vertretung der Datenschutzbelange der jeweiligen Behörde bei Kontrollen durch Revision, Wirtschaftsprüfer oder Datenschutzaufsichtsbehörden. Die vorstehend genannten Aufgaben stehen den Bestimmungen des § 7 a BremDSG teilweise sogar entgegen und beeinträchtigen somit die vom Gesetzge-

ber gewollte Aufgabenwahrnehmung der behördlichen Datenschutzbeauftragten. Auch darf der beziehungsweise dem behördlichen Datenschutzbeauftragten das Recht, sich zur Wahrnehmung ihrer beziehungsweise seiner Aufgaben an die Landesbeauftragte für Datenschutz und Informationsfreiheit zu wenden, nicht beschnitten werden. Die Festlegung eines zur Verfügung stehenden Zeitkontingents für die Erfüllung der Aufgaben der oder des behördlichen Datenschutzbeauftragten ist mit den Bestimmungen des § 7 a BremDSG ebenfalls nicht zu vereinbaren. Die behördlichen Datenschutzbeauftragten sind gemäß § 7 a Absatz 3 Satz 2 BremDSG weisungsfrei. Zur Gewährleistung ihrer Unabhängigkeit darf die Bestellung nicht zeitlich befristet werden, mindestens sind fünf Jahre vorzusehen. Auch besondere Regelungen über die Haftung der behördlichen Datenschutzbeauftragten sind mit der Weisungsfreiheit nicht zu vereinbaren.

Wir wiesen die zuständige Senatorin auf die in den Verträgen enthaltenen Regelungen, die mit § 7 a BremDSG nicht zu vereinbaren sind, hin und forderten zur Anpassung der vertraglichen Vereinbarungen an die zu beachtende Rechtslage auf.

Auch die öffentlichen Stellen im Bereich der Stadtverwaltung Bremerhaven müssen den Bestimmungen des § 7 a BremDSG entsprechen. Unter den Begriff der öffentlichen Stelle fallen im Bereich der Stadtverwaltung die einzelnen Ämter, Eigenbetriebe und Wirtschaftsbetriebe sowie die Gesellschaften der Stadt. Ihre Aufgabe ist es, die behördlichen Datenschutzbeauftragten jeweils für sich zu bestellen oder die Übertragung der Funktion unter Berücksichtigung der zu beachtenden gesetzlichen Regelungen zu beenden. Eine vom Magistrat der Stadt Bremerhaven vorgesehene Verfahrensregelung sieht hierzu vor, dass die zuständigen Dezernate, Organisationseinheiten, Wirtschaftsbetriebe und Eigenbetriebe zwar selbst bestimmen, wer die Aufgaben der oder des behördlichen Datenschutzbeauftragten wahrnehmen und das Mitbestimmungsverfahren durchführen soll. Die Bestellung, ihr Widerruf und die Meldung sollen dann aber vom Personalamt aufgrund einer Mitteilung der vorstehend genannten Stellen vorgenommen werden. Hierzu machten wir darauf aufmerksam, dass dem Personalamt von den Ämtern, Eigenbetrieben und Wirtschaftsbetrieben, auch über die Dezernentin oder den Dezernenten lediglich mitgeteilt werden kann, wer zur oder zum behördlichen Datenschutzbeauftragten bestellt wurde beziehungsweise welche Bestellung widerrufen wurde. Das Personalamt selbst darf keine Bestellung oder Beendigung für die Organisationseinheiten vornehmen. Eine personalrechtliche Grundlage für die Bestellung oder die Beendigung der Funktion der oder des behördlichen Datenschutzbeauftragten gibt es nicht. Wir forderten das Personalamt auf, die vorgesehene Verfahrensregelung zu korrigieren. Für denkbar halten wir es, dass die nach § 7 a Absatz 5 BremDSG von den öffentlichen Stellen bei der Landesbeauftragten für Datenschutz und Informationsfreiheit unverzüglich vorzunehmende Meldung der Bestellung oder Beendigung des Amtes behördlicher Datenschutzbeauftragter über das Personalamt in einer Botenfunktion erfolgt. Die Stadt Bremerhaven beharrte daraufhin auf ihrer Position, dass, da es sich um eine personalrechtliche Entscheidung handele, die Zuständigkeit für die Bestellung und den Widerruf eindeutig beim Personalamt liege. Sie halte deshalb an ihrer Auffassung fest. Wir widersprachen der Auffassung der Stadt und forderten sie nochmals auf, ihr Verfahren zu ändern.

## 4. Datenschutz durch Technikgestaltung und Technikbewertung

### 4.1 Sichere Administrationsumgebung Dataport

Nachdem wir in den vergangenen Berichtsjahren (vergleiche 33. Jahresbericht, Ziffer 4.3) auch im Zusammenhang mit der Einführung der sicheren Betriebsinfrastruktur BASIS.bremen (vergleiche 34. Jahresbericht, Ziffer 4.2) über Anforderungen hinsichtlich der Funktionalität und der Kontrolle der Administrationsumgebung berichtet hatten, haben wir in diesem Jahr den Entwurf des „Konzept Administrationsplattform für den BASIS.bremen FHB Version 1.4“ erhalten.

Bei diesem Konzept handelt es sich im Wesentlichen um eine Beschreibung der technischen Implementierung. Wir haben die Senatorin für Finanzen darauf hingewiesen, dass wir dieses Dokument nur als ergänzendes Konzept zu einem noch ausstehenden Datenschutzkonzept betrachten und darum gebeten, uns ein aussagefähiges Datenschutzkonzept zur Administrationsplattform vorzulegen. Weiterhin haben wir darauf hingewiesen, dass uns das Ergebnis einer Prüfung und Bewertung dieses Dokumentes durch die Senatorin für Finanzen als verantwortliche Stelle im

Rahmen der Auftragskontrolle nach § 9 Bremisches Datenschutzgesetz nicht vorliegt.

Wir haben deutlich gemacht, dass sich der Schutzbedarf der Administrationsplattform am Schutzbedarf der zu administrierenden Daten und Verfahren auszurichten hat. Wir gehen derzeit davon aus, dass sich das noch ausstehende Datenschutzkonzept daher am Schutzbedarf „hoch“ ausrichten muss. Des Weiteren haben wir darauf hingewiesen, dass auch die in diesem Zusammenhang angeführte eigenständige Management-Domäne im Datenschutzkonzept berücksichtig werden muss, für die hinsichtlich der datenschutzrechtlichen Anforderungen und des Schutzbedarfs die gleichen Anforderungen und Regelungen gelten wie für die Administrationsplattform selbst.

### 4.2 VISkompakt – Zentrales System zur elektronischen Aktenführung

Auch in diesem Jahr haben wir uns mit dem zentralen System zur elektronischen Aktenführung VISkompakt beschäftigt. Unsere datenschutzrechtlichen Anforderungen hatten wir bereits in den Vorjahren vorgetragen (vergleiche 32. Jahresbericht, Ziffer 4.3; 33. Jahresbericht, Ziffer 4.2 und 34. Jahresbericht, Ziffer 4.4).

In der Diskussion stehen wir derzeit insbesondere zu Fragen des Schutzbedarfs von Daten und den daraus resultierenden Maßnahmen, wie zum Beispiel der Verschlüsselung von Daten. Weiterhin offen sind Fragen zur revisionssicheren Protokollierung auf Anwendungsebene und Administrationsebene und besonders auch der Mandantentrennung. Daneben sind weiterhin Detailfragen ungeklärt, beispielsweise die lückenlose Aufrechterhaltung der Zugriffskontrolle bei Löschvorgängen, wenn mehrere verantwortliche Stellen einen gemeinsamen Mandanten benutzen.

Wie wir bereits im letzten Jahresbericht dargelegt hatten, muss bei der Verarbeitung von personenbezogenen Daten innerhalb der Verwaltung davon ausgegangen werden, dass vielfach sensible personenbezogene Daten betroffen sind. Dazu gehören beispielsweise Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeiten, Gesundheitsdaten und Sexualdaten. Auch bei Daten von Sicherheitsbehörden ist in der Regel mindestens vom Schutzbedarf „hoch“ auszugehen. Unter anderem ist daher das Schutzziel Vertraulichkeit besonders zu beachten. Es sind besondere Maßnahmen zu treffen, um dem Schutzbedarf dieser Daten gerecht zu werden. Damit VISkompakt also eine breite Anwendung finden kann, sollten die zu treffenden technischen und organisatorischen Maßnahmen am Schutzbedarf „hoch“ für die personenbezogenen Daten ausgerichtet werden. Zu diesem Zweck sind insbesondere Maßnahmen zur Verschlüsselung der Daten sowohl auf dem Übertragungsweg als auch der Inhaltsdaten und Metadaten zu treffen. In diesem Zusammenhang spielt die Wahrung von Berufsgeheimnissen und Verschwiegenheitspflichten eine wichtige Rolle. Weiterhin erwarten wir die Ausgestaltung einer revisionssicheren Protokollierung auf Anwendungsebene und Administrationsebene.

Die bereits für Anfang des Jahres angekündigten angepassten Unterlagen zur Datenschutzdokumentation sind auch nach Nachfrage bisher nicht bei uns eingegangen. Somit müssen wir wie im vergangenen Berichtsjahr aufgrund der Dokumentenlage davon ausgehen, dass das System VISkompakt nur für Daten mit dem Schutzbedarf „normal“ verwendet werden kann. Die teilnehmenden Dienststellen haben daher vor Einsatz von VISkompakt zwingend eine Schutzbedarfsfeststellung für die zu verarbeitenden personenbezogenen Daten vorzunehmen. Sofern dabei der Schutzbedarf „hoch“ und „sehr hoch“ festgestellt wird, muss derzeit auf einen Einsatz von VISkompakt verzichtet werden.

Besondere Probleme sehen wir auch bei der Mandantentrennung. Die konkreten Planungen für den flächendeckenden Einsatz von VISkompakt sehen vor, dass innerhalb von VISkompakt möglichst wenig sogenannte Mandanten genutzt werden. Dabei wird von dem Modell ausgegangen, dass je Ressort in der Regel lediglich ein einzelner Mandant betrieben wird. Wir haben hingegen erhebliche Zweifel an der datenschutzrechtlichen Zulässigkeit der Nutzung nur eines Mandanten je Ressort für die Freie Hansestadt Bremen (FHB). Vielmehr gehen wir zurzeit davon aus, dass für jede Verantwortliche Stelle gemäß § 2 Absatz 3 Nummer 1 Bremisches Datenschutzgesetz (BremDSG) ein Mandant einzurichten ist.

Zur Abschätzung der datenschutzrechtlichen Zulässigkeit sind die folgenden Rahmenbedingungen aus dem BremDSG zu beachten:

Nach § 7 Absatz 4 Nummer 8 BremDSG ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden können (Trennungsgebot).

Gemäß § 7 Absatz 4 Nummer 3 BremDSG ist zu gewährleisten, dass die zur Nutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, der Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle).

Die Anforderungen an die sogenannte Weitergabekontrolle bei der Verarbeitung personenbezogener Daten regelt § 7 Absatz 4 Nummer 4 BremDSG. Danach ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist. Auch ist das Verhältnismäßigkeitsprinzip (§ 7 Absatz 1 Satz 2 BremDSG) zu beachten.

Diese Anforderungen lassen sich mit VISkompakt nach unserem derzeitigen Kenntnisstand nur dann abschließend durchhalten, wenn je verantwortlicher Stelle ein Mandant eingesetzt wird. Insbesondere muss zumindest eine vollständige logische Trennung möglich sein. Die Trennung ist technisch zu gewährleisten. Diese technischen Datenschutzmaßnahmen müssen insbesondere eine Trennung der Daten auf den Ebenen der Datenhaltung, der Datenverarbeitung und des Datentransports sicherstellen. Die logische Trennung vollständig wie geplant durch die reine Anwendung von Rechten und Rollen und die Nutzung verschiedener Ablagen innerhalb eines Mandanten gewährleisten zu können, erscheint unwahrscheinlich. Auch die innerhalb von VISkompkat zur Verfügung stehenden Protokollierungsmöglichkeiten stehen dem entgegen. Nach unserem derzeitigen Kenntnisstand lässt sich mit den in VISkompakt vorhandenen Methoden zur Protokollierung keine Trennung der Protokolldaten hinsichtlich der jeweiligen verantwortlichen Stelle erreichen. In diesem Zusammenhang ist nach unserer derzeitigen Auffassung die Tätigkeit der Administratoren für den Anwendungsfall „Datenverarbeitung mehrerer verantwortlicher Stellen innerhalb eines VIS-Mandanten“ nicht ausreichend protokolliert, um eine vollständige, lückenlose Protokollierung der Zugriffsberechtigungen und Zugriffe zu erhalten und damit etwaige unberechtigte Nutzungen nachweisen zu können. Hingegen lässt sich eine möglichst vollständige, lückenlose und bezogen auf die verantwortlichen Stellen unvermischte Protokollierung nach unserer Auffassung nur über die Nutzung (mindestens) eines Mandanten je teilnehmender Dienststelle, also der verantwortlichen Stelle, realisieren. In Sonderfällen sind durchaus auch mehrere Mandanten je verantwortlicher Stelle denkbar.

Dem geplanten flächendeckenden Einsatz von VISkompakt sehen wir in der Variante mit nur wenigen, ressortbezogenen Mandanten insgesamt kritisch entgegen, nicht zuletzt, weil VISkompakt aus verschiedenen Gründen im alten Active Directory (Verzeichnisdienst) betrieben wird (siehe auch Ziffer 4.7 dieses Berichts).

### 4.3 Verarbeitung von Dateien im Zahlungsverkehr

Aufgrund des Projekts „Schnittstelle Ausgaben Stammdatenkreditor“ haben wir uns auch mit der Verarbeitung von Dateien im Zahlungsverkehr befasst und dabei mehrfach Stellung genommen zum Verfahren TransX der Landeshauptkasse. Dieses Programm verarbeitet Kassendaten wie zum Beispiel Einnahmedateien, Ausgabedateien und Giro-Dateien, die an nachfolgende Verfahren wie SAP und Giro weitergegeben werden.

Nachbesserungsbedarf beziehungsweise Änderungsbedarf sehen wir vornehmlich im Bereich der Authentifizierung sowie der Protokollierung. Wir gehen davon aus, dass unsere Hinweise spätestens im Rahmen des Projekts SEPA (Single Euro Payments Area) (vergleiche Ziffer 10.2 dieses Jahresberichts) umgesetzt werden.

### 4.4 BASIS.Bremen – Standardisierung der Infrastruktur

Im März des Berichtsjahres wurde die Projektorganisation zur zentralisierten und standardisierten Betriebsorganisation für die Verwaltungsarbeitsplätze im Informationstechnik-Ausschuss (ITA) der bremischen Verwaltung vorgestellt. Die Bearbei-

tung des Themas Datenschutz und Datensicherheit wurde im Rahmen eines speziellen Arbeitspakets mit dem Projektstart entsprechend der Zusage des Senats zu unseren Ausführungen im 34. Jahresbericht (vergleiche Ziffer 4.2 zur sicheren Betriebsinfrastruktur) offiziell begonnen. Dieses Arbeitspaket sollte projektübergreifende Themen zum Datenschutz und zur Datensicherheit bearbeiten. Wir erwarteten deshalb den dringend erforderlichen Beginn einer standardisierten Vorgehensweise zur Entwicklung tragfähiger Datenschutzprozesse und Datensicherheitsprozesse. Dazu gehört ein qualifiziertes Sicherheitskonzept für das Projekt selbst, aber auch die Lösung offener Themen der technischen Infrastruktur insgesamt, in die das Projekt eingebettet ist. Diese Themen sind über mehrere Jahre immer wieder von uns, verbunden mit entsprechenden Anforderungen, erörtert worden. Als Beispiele hierzu seien Sicherheitsanforderungen an die administrativen Zugänge in das Bremer Verwaltungsnetz (vergleiche 31. Jahresbericht, Ziffer 6.4; 32. Jahresbericht, Ziffer 4.2; 33. Jahresbericht, Ziffer 4.3 und 35. Jahresbericht, Ziffer 4.1 ), die Entwicklung eines Konzepts zum Sicherheitsmanagement und damit verbundene Themen zur Möglichkeit der Wahrnehmung datenschutzrechtlicher Verantwortlichkeit in verteilten Systemen (vergleiche 32. Jahresbericht, Ziffer 4.1 und 33. Jahresbericht, Ziffer 4.4) und die Schaffung der dafür erforderlichen Grundlagen wie die Durchführung einer Risikoanalyse genannt.

Die Entwicklung der erforderlichen Datenschutzkonzepte und Datensicherheitskonzepte ist bis jetzt, von wenigen Ausnahmen abgesehen, nicht erfolgt. In seiner Antwort zu unserem 32. Jahresbericht ging der Senat bereits davon aus, dass die Entwicklung einer datenschutzgerechten administrativen Umgebung (hier: administrativer Zugang am Dataport-Standort Bremen) 2010 abgeschlossen wäre. In unserem aktuellen Jahresbericht (vergleiche Ziffer 4.1 Administrationskonzept Dataport) wird deutlich, dass selbst für diesen zentralen Bereich noch kein Datenschutzkonzept zur Verfügung steht und noch wesentliche Fragen offen sind.

Wir haben deshalb unsere Anforderungen an das Projekt BASIS.Bremen noch einmal zusammengefasst und an die Senatorin für Finanzen übermittelt. Es wurden unter anderem eine geeignete Vorbereitung der Migration und ein entsprechendes Risikomanagement, die Gewährleistung der sicheren Anbindung dezentraler Standorte, die Schaffung einer zentralen Managementstruktur, die Dokumentation der Sicherheitseinstellungen im Active Directory (Verzeichnisdienst) insbesondere für die Organisationseinheit Dataport genannt. Außerdem forderten wir beispielsweise eine vollständige Strukturanalyse, Risikoanalyse und Schutzbedarfsfeststellung, eine datenschutzkonforme Konzeption und einen entsprechenden Betrieb der Administrationsplattform für die Bremer Systeme, den datenschutzgerechten Einsatz administrativer Werkzeuge (die unterhalb von Berechtigungsstrukturen, die den Zugriff auf personenbezogene Daten steuern, arbeiten) und Auditierungskonzepte und Revisionskonzepte zur Gewährleistung der Transparenz der Datenzugriffe und Verarbeitungsprozesse.

Eine inhaltliche Antwort auf unsere datenschutzrechtlichen Anforderungen wurde uns bis zum Oktober des Berichtsjahres angekündigt. Bisher sind uns bis auf das Sicherheitskonzept zum Active Directory (AD), dass immer noch keine Festlegungen zur Protokollierung und Revision enthält, überwiegend technische Beschreibungen zu einzelnen Themen des Dienstleisters Dataport übergeben worden. Eine Bewertung hinsichtlich der Qualität dieser Dokumente und eine Positionierung der Senatorin für Finanzen als verantwortliche Stelle liegen uns nicht vor. Voraussetzung für eine datenschutzrechtliche Bewertung durch uns ist aber, dass die Senatorin für Finanzen als verantwortliche Stelle eine Prüfung der Dokumente von Dataport vorgenommen hat (Auftragskontrolle gemäß § 8 Bremisches Datenschutzgesetz). Wir haben sie deshalb gebeten, uns zukünftig nur noch inhaltlich geprüfte Unterlagen mit dem Ergebnis ihrer Prüfung und den sich daraus möglicherweise ergebenden Fragen zu übersenden.

Bis heute fehlen die zentralen Datenschutzkonzepte. Die vom Senat in seiner Antwort zu unserem 33. Jahresbericht geäußerte Auffassung, dass die Einführung des Verwaltungs-PC (jetzt BASIS.Bremen) mit seinen standardisierten Betriebsabläufen einen erheblichen Sicherheitsgewinn darstellt, ist momentan nicht nachvollziehbar. Die Anforderung, dass darauf die von uns genannten weiteren Schritte aufsetzen sollen, ist nicht erfüllt.

Im November erklärte die Senatorin für Finanzen, dass sie externe Unterstützung vom Institut für Informationsmanagement Bremen GmbH zur Bearbeitung der The-

men „zentrale Zugriffsinfrastruktur“ und „Administrative Tätigkeiten“ in Anspruch nehmen will. Dennoch gehen wir davon aus, dass einige Pilotprojekte abgeschlossen und in den Echtbetrieb überführt sein werden, ohne dass uns aussagefähige Datenschutzkonzepte und Datensicherheitskonzepte entsprechend unseren mehrfach formulierten Anforderungen vorgelegt wurden. Unter Berücksichtigung der langen Zeiträume, die bis jetzt zur Lösung zumindest einiger zentraler Fragen zur Verfügung gestanden haben, befürchten wir, dass uns zeitnah keine der erforderlichen Konzeptionen vorliegen werden. Deshalb werden wir zunächst auf eine erneute Darstellung unserer Anforderungen verzichten. Aufgrund seiner zentralen Bedeutung werden wir das Projekt weiter begleiten, sobald uns von der Senatorin für Finanzen die ausstehenden und von ihr qualitativ geprüften Konzepte zur Verfügung gestellt werden. Bis dahin fehlen für eine weitere Begleitung unsererseits die inhaltlichen Voraussetzungen.

### 4.5 Einsätze von Smartphones und Tablet-Computer in der bremischen Verwaltung

Tablet-Computer (englisch: tablet, „Schreibtafel“) sind leichte, tragbare Computer mit Touchscreen-Display (Sensorbildschirm). Sie ähneln im Leistungsumfang den Smartphones. Die folgenden Ausführungen zu Smartphones gelten deshalb entsprechend.

Mit Smartphones können wir mobil telefonieren, Kurznachrichten (SMS, Abkürzung für Short Message Service) und multimediale Kurznachrichten (MMS, Multimedia Message Service) verschicken. Im Gegensatz zum Handy haben sie ein eigenes Betriebssystem. Diese Betriebssysteme ermöglichen es den Nutzerinnen und Nutzern, Anwendungen (Apps, Kurzform von Applications [Anwendungen]) nachträglich zu installieren. Smartphones sind multimediafähig, verfügen über ein Global Positioning System (globales Navigationssatellitensystem) und können sich mit dem Internet verbinden. Smartphones sind ausgestattet mit Terminverwaltung und Adressverwaltung, Textverarbeitung, Tabellenkalkulation, Aufgabenlisten und lassen sich mit PC-Applikationen, wie zum Beispiel Outlook oder Office, über universelle Schnittstellen (USB) oder Funknetze (WLAN) synchronisieren. Außerdem gibt es eine Vielzahl von Einstellungsmöglichkeiten.

Die vielfältigen Nutzungsmöglichkeiten und die Anbindung von Smartphones an das Bremer Verwaltungsnetz (BVN) werden auch in der bremischen Verwaltung nachgefragt. Deshalb initiierte die Senatorin für Finanzen im Berichtsjahr ein Vorprojekt „Mobile Connection (mobile Verbindung)“ und legte für die Teilnahme an dem Projekt im Januar des Berichtsjahres einen Verfahrensablauf fest. Dieser Ablauf beinhaltet im Wesentlichen Regeln zur Einrichtung und Nutzung der Zugänge zum Bremer Verwaltungsnetz. Darin wurden insbesondere die zugelassenen Endgeräte (iPhone, iPad und Windows Phone) und ein geregeltes Antragsverfahren für die Einwahl in das Verwaltungsnetz beschrieben. Der inhaltliche Schwerpunkt des Verfahrensablaufs liegt auf der technischen Gestaltung insbesondere zur Synchronisation von dienstlichen Maildaten, Kalenderdaten und Kontaktdaten über die Synchronisationsdienste des zentralen Exchange-Systems des Bremer Verwaltungsnetzes. Die Verantwortung für die Sicherheit der Geräte sowie der darauf gespeicherten Daten wird der den Zugang zum BVN beantragenden Person übertragen. Datenschutzaspekte beschränken sich auf einzelne Maßnahmen (wie etwa die Regelung des Zugriffs auf die Dienste des Exchange-Systems über technische Einstellungen) und den Hinweis, dass keine personenbezogenen Daten verarbeitet werden. Der Informationstechnik-Ausschuss (ITA) der bremischen Verwaltung befasste sich in diesem Jahr dreimal mit diesem Vorprojekt. Zentrale Themenbereiche waren auch hier Gestaltungsfragen zur technischen Machbarkeit.

Mit dem Einsatz der Smartphones sind Risiken für die Datensicherheit verbunden. Auf einem Workshop des Arbeitskreises Technik der Datenschutzbehörden erläuterte ein Mitarbeiter vom Testlabor Mobile Sicherheit des Fraunhofer Instituts insgesamt 15 Angriffsvektoren auf logischer und physischer Ebene, die verschiedene Zugangsmöglichkeiten für mögliche Angriffe beschreiben. Zugänge können auf der logischen Ebene beispielsweise die Kommunikationsdienste, der Browser, das Betriebssystem und natürlich die Apps sein. Benutzer und Benutzerinnen können in der Regel die echte Funktionalität der Anwendungen nicht kontrollieren. Viele Apps verschicken Zusatzinformationen, die für die Durchführung der geladenen Anwendung nicht erforderlich sind. Es ist den Benutzerinnen und Benutzern nicht möglich, zu überprüfen, ob die Apps eine Weitergabe personenbezogener Daten (wie

etwa Maildaten, Kalenderdaten und Kontaktdaten oder auch der IMEI (eindeutiger Identifier, den jedes Smartphone besitzt) und Profilbildungen, eventuell zusätzlich durch eine Verknüpfung mit gespeicherten Geodaten, vornehmen. Darüber hinaus sind allgemein bekannte Manipulationsmöglichkeiten an der Firmware (Software, die funktionell direkt mit der Hardware verbunden ist und eine Position zwischen den physikalischen Komponenten und der Anwendungssoftware einnimmt) mit Hilfe eines „Jailbreak“ („Gefängnisausbruch“) möglich. Die Firmware wird modifiziert, sodass beispielsweise Software von verschiedenen Quellen auf das Gerät installiert werden kann. Stiftung Warentest testete im November 2012 Shopping Apps (12 Apps zum Einkaufen, 25 „Einkaufshelfer“) unter anderem mit dem Ziel, ob sie sensible Daten ungefragt an Dritte übermitteln. Ihr Ergebnis: nur zwei davon waren sicher und gut. In einem Test im Mai 2012 stufte die Stiftung Warentest von 63 geprüften Anwendungen 28 als kritisch unter Datenschutzgesichtspunkten ein. Weitere bekannte Programme wurden sogar als sehr kritisch eingestuft, beispielsweise die App „Foodspotting“, die nicht nur die Suche nach leckerem Essen unterstütze, sondern auch alle auf den Smartphones gespeicherten Mailadressen in die Vereinigten Staaten von Amerika (USA) übermittele. Apps von sozialen Netzwerken holten sich auf den Smartphones gespeicherte Kontaktdaten (Name, Telefonnummern, E-Mail-Adressen). Auch Passwörter würden im Klartext an die Server der jeweiligen Anbieter teilweise übermittelt (vergleiche Zeitschrift Test, Ausgabe 6/12).

Durch die gleichzeitige Kopplung des Smartphones mit verschiedenen Umgebungen wie etwa dem Verwaltungsnetzwerk und Datenverarbeitungsinfrastrukturen von anderen Anbietern, die eventuell auch privat genutzt werden (beispielsweise soziale Netzwerke, Clouddienste [Dienste, die im Internet bereitgestellt werden]), ist von einer großen Angriffsfläche auszugehen und von einem hohen Risiko des ungewollten Abfließens von dienstlichen Daten. Auch wenn der Aufwand, über diese Zugänge unzulässige Zugriffe auf die Systeme zu erlangen und die sich daraus ergebenden Manipulationsmöglichkeiten verschieden sind, weist allein die Anzahl der Angriffspunkte darauf hin, dass die Gewährleistung von Datenschutz und Datensicherheit einen hohen Aufwand erfordert. Diese kurze Skizzierung macht bereits deutlich, dass für den Zugriff von Smartphones auf Daten und Dienste des BVN vorab eine umfassende Betrachtung der Risikofaktoren erforderlich ist.

Momentan werden jedoch Anträge auf Verbindungen mobiler Geräte zum BVN (Mobile Connection [Verbindung] FHB) angenommen und bearbeitet, obwohl das Verfahren erst im Rahmen eines „Vorpilotprojektes“ getestet werden soll. Die Übertragung der Verantwortlichkeit für die sichere Konfiguration dienstlicher Geräte auf die Nutzerinnen und Nutzer, wie sie im Verfahrensablauf der Senatorin für Finanzen festgelegt wurde, ist nicht möglich. Da die Geräte bereits eingesetzt sind, hätten die entsprechenden Analysen zumindest Teil des „Vorpilotprojektes“ sein müssen. Ziel des Pilotprojektes muss es jetzt sein, die Risiken zu analysieren, eine Entscheidung über Einsatzszenarios zu treffen, die erforderlichen Sicherheitsmaßnahmen auf den Endgeräten und für das BVN festzulegen und auf ihre Wirksamkeit für den Einsatz und im laufenden Betrieb zu prüfen. Es muss eine klare Bewertung des Restrisikos vorliegen, aufgrund derer ein transparenter Abwägungsprozess zwischen gewünschten Funktionalitäten und Sicherheit stattfinden kann. Voraussetzung für einen sicheren Betrieb ist ein funktionierendes Informationstechnologie-Sicherheitsmanagement für das Land Bremen (vergleiche 32. Jahresbericht, Ziffer 4.1).

### 4.6 Orientierungshilfe Mandantentrennung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschäftigte sich über ihren Arbeitskreis Technik mit dem Thema Mandantentrennung und veröffentlichte eine Orientierungshilfe hierzu. An der Orientierungshilfe arbeiteten wir mit.

Aufgrund vielfältiger Erfahrungen aus der Prüftätigkeit und Beratungstätigkeit der Datenschutzbeauftragten des Bundes und der Länder erwies es sich als zwingend notwendig, eine Einordnung des Themas Mandantentrennung aus Sicht des Datenschutzes zu geben, weil keine eindeutige Definition des Begriffes Mandant existiert. Dennoch wird er in unterschiedlichen Datenverarbeitungskontexten in großer Regelmäßigkeit verwandt – mit unterschiedlichen Bedeutungen. Dabei macht aber gerade die uneinheitliche Interpretation des Begriffs erhebliche Schwierig-

keiten. Insgesamt werden immer mehr kooperative Betriebsmodelle für Datenverarbeitungssysteme angewandt, um Hardware und Software möglichst effektiv und kostengünstig zu nutzen. Die gemeinsame Nutzung solcher Infrastrukturen unterliegt aber erhöhten Anforderungen an die Trennung der personenbezogenen Daten. Die aus der gemeinsamen Nutzung der Daten entstehenden Risiken sind technisch hinreichend zu reduzieren; die gesetzlichen Anforderungen zur getrennten Verarbeitung von zu unterschiedlichen Zwecken erhobenen personenbezogenen Daten müssen erfüllt werden. Die Orientierungshilfe Mandantentrennung konkretisiert den Begriff Mandant und zeigt die aus Datenschutzsicht notwendigen Schritte zur Prüfung einer ausreichenden Trennung von automatisierten Verfahren bei der Nutzung einer gemeinsamen Informationstechnologie-Infrastruktur auf.

### 4.7 Passwortrichtlinie für altes AD

Für die Verwaltung großer Datenverarbeitungsnetzwerke wie es das Bremer Verwaltungsnetz (BVN) ist, werden sogenannte Verzeichnisdienste genutzt. Verzeichnisdienste erlauben die zentrale Verwaltung aller am Netzwerk beteiligten Objekte wie etwa der angeschlossenen Geräte, der genutzten Programme oder Benutzerkonten. Im BVN werden derzeit zwei derartige Verzeichnisdienste parallel genutzt. Dabei handelt es sich um Verzeichnisdienste, die von der Firma Microsoft entwickelt wurden und Active Directory (AD) als Produktnamen tragen. Das „alte“ AD ist ein Verzeichnisdienst, der vor ein paar Jahren technisch aufgebaut wurde und damals als alleiniger, zentraler Verzeichnisdienst für das BVN gedacht war. Allerdings hat dieses AD niemals einen anderen Status als „im Testbetrieb“ erreicht. Unter anderem sind es datenschutzrechtliche Bedenken, die dem Echtbetrieb entgegen stehen. Näheres hierzu ist unserem 29. Jahresbericht unter der Ziffer 6.4 zu entnehmen.

Im Zuge der E-Mail-Migration wurde parallel zum alten AD ein weiteres AD aufgebaut (siehe 31. Jahresbericht, Ziffer 6.5), der Verzeichnisdienst für den Echtbetrieb. Jedoch kann nach wie vor das alte AD nicht abgeschaltet werden, da viele Anwendungen innerhalb des BVN auf diesen Verzeichnisdienst angewiesen sind. Das alte AD befindet sich somit quasi im Echtbetrieb. Im Rahmen verschiedener Projekte sind wir im Berichtsjahr darauf aufmerksam geworden, dass für das alte AD des BVN die aktuelle, seit Juli 2011 gültige Kennwortrichtlinie, nicht technisch umgesetzt ist. Zusätzlich zu dem aus Datenschutzsicht äußerst unbefriedigenden Umstand des Quasi-Echtbetriebs wird dadurch kein durchgehender Standard für Passwörter oder Kennwörter im BVN erreicht.

So können innerhalb des alten AD Passwörter verwendet werden, die aus mindestens sechs Zeichen bestehen. Die aktuelle Kennwortrichtlinie schreibt aber für die Länge von Kennwörtern mindestens acht Zeichen vor. Wir haben dies gegenüber der Senatorin für Finanzen moniert und gefordert, dass die Kennwortrichtlinie ebenfalls für das alte AD gelten müsse und dass die Geltung der Kennwortrichtlinie selbstverständlich auch technisch erzwungen werden muss. Eine rein organisatorische Regelung hierzu reicht nicht aus. Diese Forderung ist vor dem Hintergrund, dass viele sensible Bereiche der bremischen Verwaltung das alte AD nutzen, verhältnismäßig. Die Senatorin für Finanzen hat uns mitgeteilt, dass die von uns geforderte technische Maßnahme durchgeführt werde und dass dies nach rechtzeitiger Ankündigung über den Informationstechnologie-Ausschuss (ITA) innerhalb des ersten Quartals 2013 erfolgen werde.

### 4.8 Bericht aus dem Arbeitskreis Technik

Zentrale Themen des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder waren im Berichtsjahr unter anderem die Erstellung einer Orientierungshilfe zum Thema Mandantentrennung (siehe Ziffer 4.6 dieses Berichts) sowie ein technisch-juristisch interdisziplinärer Workshop zu dem aus der Perspektive des Datenschutzes als sehr kritisch zu bewertenden Thema „Bring Your Own Device“, abgekürzt als BYOD.

Bei BYOD geht es darum, dass Mitarbeiterinnen und Mitarbeiter eigene, private Endgeräte mit in die Organisationen bringen und für dienstliche Belange nutzen. Dabei kann es sich beispielsweise um sogenannte Smartphones (Mobiltelefone, die über viele Computerfunktionalitäten verfügen; sie sind quasi tragbare Computer) oder Tablet-Computer (tragbare, flache Computer die in der Regel durch Gesten der Benutzerinnen und Benutzer gesteuert werden) handeln. Die Geräte können

in vielfältiger Art und Weise an die Informationstechnologie-Infrastrukturen der Organisationen angebunden werden und ermöglichen damit eine Nutzung organisationsinterner Daten und Infrastrukturen. Datenschutzrechtlich kritisch ist dabei, dass zu diesem Zweck die Netzwerke der Organisationen geöffnet werden. Zwar kann dies über definierte und somit kontrollierbare Wege erfolgen, das Problem sind aber die privaten Endgeräte selbst. Die Organisationen können in der Regel keine administrative Hoheit über das Endgerät selbst und damit über die dort konfigurierten Sicherungsmaßnahmen erhalten. Personenbezogene Daten, für die die Organisation verantwortlich ist, werden also plötzlich in einem potenziell unsicheren, weil nicht kontrollierbaren Umfeld genutzt und verarbeitet. Somit können besonders die technischen Anforderungen zum Schutz personenbezogener Daten gemäß § 7 Bremisches Datenschutzgesetz nicht erfüllt werden. Im Workshop wurde eine differenzierte rechtliche und technische Einordnung von BYOD-Bestrebungen vorgenommen. Ergebnis der Workshops ist, dass BYOD immer ein Risiko birgt, da die Organisation niemals die volle Kontrolle über die Endgeräte und die damit zu verarbeitenden personenbezogenen Daten erhalten kann. Somit ist von BYOD-Bestrebungen abzusehen.

## 5. Inneres

### 5.1 Einführung eines Terminmanagements in der bremischen Verwaltung

Beim Senator für Inneres und Sport ist ein Projekt zur Einführung eines Terminmanagements in der bremischen Verwaltung gestartet. Das internetbasierte Verfahren soll bereits vorhandene Anwendungen einbinden oder ersetzen. Durch ein einheitliches System zur Terminvergabe und Erteilung von Auskünften per Telefon, E-Mail oder über das Internet sollen die Servicequalität für die Bürgerinnen und Bürger verbessert und Wartezeiten verkürzt werden.

Für die Ausschreibung des Verfahrens wurde von der Projektgruppe eine Leistungsbeschreibung angefertigt und von der Landesbeauftragten für Datenschutz und Informationsfreiheit unter datenschutzrechtlichen Gesichtspunkten geprüft. Ausgeschrieben werden soll ein Rahmenvertrag zum Betrieb eines Systems zur Terminvereinbarung und Kundensteuerung. Wir wiesen den Senator für Inneres und Sport darauf hin, dass zum Zeitpunkt der Bewertung der auf die Ausschreibung eingehenden Angebote ein Datenschutzkonzept vorliegen muss, denn bei der Auswahl des Auftragnehmers muss auch geprüft werden, ob dieser die datenschutzrechtlichen Anforderungen umsetzen kann. Wir machten deutlich, dass – sofern das Verfahren als integriertes System laufen soll – die Abschottung des Terminmanagements gegenüber dem Rest des Systems besonderer Aufmerksamkeit bedarf. Möglichst frühzeitig sollte ein zumindest grobes Rollenkonzept und Rechtekonzept erstellt werden. Zudem hielten wir eine Ergänzung der in der Leistungsbeschreibung aufgeführten technischen und organisatorischen Maßnahmen um die Punkte „Zugriffskontrolle der Mitarbeiter“ und „Eingabekontrolle“ (Protokollierung der Zugriffe) für erforderlich. Wir werden das Projekt weiterhin begleiten.

### 5.2 Elektronisches Personenstandsregister

Die Länder Hamburg, Schleswig-Holstein und Bremen haben im Jahr 2011 ein gemeinsames elektronisches Personenstandsregister eingeführt, das technisch von der Anstalt öffentlichen Rechts Dataport betrieben wird. Datenschutzrechtlich wird das Projekt von den Landesbeauftragten aus Schleswig-Holstein und Hamburg sowie der Landesbeauftragten aus Bremen gemeinsam betreut. Das größte datenschutzrechtliche Problem sahen wir in der mangelhaften Protokollierung und in der unzureichenden Mandantentrennung. Wir bemängelten, dass keine aussagekräftigen Protokolle geschrieben wurden, anhand derer beispielsweise überprüft und festgestellt werden konnte, ob die Nutzerinnen und Nutzer des Verfahrens lediglich auf die ihnen zuzuordnenden Daten Zugriff haben oder hatten. Die Eingabekontrolle selbst war ebenfalls anhand der Protokolldaten nicht möglich. Wir vertraten die Auffassung, dass die Protokolldaten immer bezogen auf das jeweilige Bundesland zu schreiben sind. Zudem forderten wir, dass ein länderübergreifender Zugriff auf personenbezogene Daten verhindert werden muss. Das bedeutet, dass die Daten für jedes Bundesland in einem gesonderten, logisch abgeschlossenen Mandanten gespeichert und verarbeitet werden müssen, was bei der vorgesehenen Haltung der Daten in einem Datenpool nicht der Fall ist. Das ist besonders heikel, da es sich um Daten aus drei Bundesländern handelt und somit auch drei verschiedene Lan-

desdatenschutzgesetze Anwendung finden würden. Die Abstimmungen der genannten Datenschutzbeauftragten der beteiligten Länder führten dazu, dass der Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe zum Thema Mandantentrennung erarbeitete (siehe Ziffer 4.6 dieses Berichts), in der aus datenschutzrechtlicher Sicht sowohl definiert wird, was Mandantentrennung bedeutet, als auch welche Prüfschritte aus Datenschutzsicht notwendig sind, um eine ausreichende Trennung der Mandanten voneinander zu erreichen. Auf dieser Basis wurde eine Änderung des elektronischen Personenstandsregisters beauftragt, die technisch sicherstellt, dass Schreibrechte und Leserechte auf die Datenbestände der beteiligten Bundesländer voneinander getrennt bleiben.

### 5.3 Kundenaufrufsysteme in den BürgerServiceCentern

Wir erhielten Eingaben von einigen Petentinnen und Petenten, die sich über das Aufrufsystem in den BürgerServiceCentern beschwerten. Sie monierten, dass auf den für alle anwesenden Bürgerinnen und Bürger sichtbaren Anzeigetafeln ihre Namen angezeigt wurden, ohne dass zuvor bei der Anmeldung ihre Einwilligung dafür eingeholt worden war. Auf Nachfrage wurde uns von den BürgerService Centern mitgeteilt, dass eigentlich am Empfang ein Hinweis auf die Anzeige erfolgen solle und auch die Option bestünde, sich unter einem Pseudonym aufrufen zu lassen. Offenbar wurde dieser Hinweis in der Praxis aber oft vergessen. Wir schrieben deshalb die Leitung des Stadtamtes mit der Bitte an, die zuständigen Mitarbeiterinnen und Mitarbeiter am Empfang beispielsweise mit Hilfe eines Rundschreibens darauf hinzuweisen, dass eine Anzeige des Namens nur aufgrund einer Einwilligung der Betroffenen erfolgen darf und dass die Bürgerinnen und Bürger im Vorfeld über eine alternative Aufrufmöglichkeit informiert werden müssen. Wir gehen davon aus, dass nun die datenschutzrechtlichen Anforderungen beachtet werden, denn seit unserem Schreiben sind bei uns keine entsprechenden Beschwerden mehr eingegangen.

### 5.4 Fortentwicklung des Meldewesens

Seit der im Jahr 2006 in Kraft getretenen Föderalismusreform ist das Meldewesen nicht mehr Länderangelegenheit, sondern unterliegt der Gesetzgebungskompetenz des Bundes. Deshalb sollte ein Bundesmeldegesetz verabschiedet werden, das die Meldegesetze der Länder ablösen wird. Ein Regierungsentwurf wurde Ende des Jahres 2011 dem Bundestag zur Beratung vorgelegt. In Kraft treten sollte das Gesetz Ende 2014. Vorher musste der Bundesrat zugestimmt haben. Der erste Entwurf, der zwar auch einige datenschutzrechtliche Defizite aufwies, sah immerhin vor, dass Daten für Werbung und Adresshandel sowie Auskünfte zu Namen und Adressen nur nach vorheriger Zustimmung der Betroffenen herausgegeben werden durften. Aufgrund des Protestes von Inkassounternehmen und Auskunfteien wurde diese datenschutzfreundliche Einwilligungslösung vom Innenausschuss des Bundestages in eine aus datenschutzrechtlicher Sicht bedenkliche Widerspruchslösung geändert. Im Juni 2012 wurde der geänderte Entwurf im Bundestag angenommen, obwohl das Plenum mit nur 26 anwesenden Abgeordneten nicht beschlussfähig war. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder kritisierte das Gesetz in ihrer Stellungnahme vom Sommer 2012 scharf und forderte den Bundesrat auf, der verabschiedeten Fassung nicht zuzustimmen. Sie forderte beispielsweise Änderungen bei der Bildung und Verwendung von Ordnungsmerkmalen und bei dem Auskunftsanspruch der betroffenen Personen. Bei den Melderegisterauskünften sollen danach die Rechte der Betroffenen deutlich gestärkt werden, beispielsweise indem für Zwecke der Werbung und des Adresshandels anstatt einer Widerspruchslösung eine Einwilligungslösung gewählt wird. Die Konferenz der Datenschutzbeauftragten sprach sich zudem gegen die Wiedereinführung einer Mitwirkungspflicht von Vermietenden bei der Anmeldung und Abmeldung der Mieterinnen und Mieter sowie für die Abschaffung der Hotelmeldepflicht aus. Nachdem einige Länder Änderungswünsche angekündigt hatten, rief der Bundesrat den Vermittlungsausschuss an. Es bleibt abzuwarten, wie das zukünftige Meldegesetz letztlich aussehen wird.

### 5.5 Aktuelle Situation im Stadtamt

In den vorherigen Jahresberichten hatten wir bereits auf die aus datenschutzrechtlicher Sicht unbefriedigende Situation im Stadtamt hingewiesen. Die Vielzahl der diesbezüglich laufenden Verfahren erfordert eine intensive Betreuung und Be-

arbeitung der offenen datenschutzrechtlichen und datenschutztechnischen Fragestellungen durch die dortigen Verantwortlichen. Aber auch für zukünftige Neueinführungen und Änderungen von Verfahren muss der datenschutzgerechte Betrieb gewährleistet werden. Doch die aktuelle Personalsituation im Stadtamt führte im vergangenen Jahr dazu, dass kaum Fortschritte in der Erstellung der ausstehenden Datenschutzkonzepte erzielt werden konnten. Da aktuell keine ausreichenden personellen Kapazitäten im Stadtamt vorhanden sind, werden auch die eingeführten quartalsweise stattfindenden Gespräche (vergleiche 34. Jahresbericht, Ziffer 5.11) derzeit ausgesetzt. Aus dieser Situation folgt, dass eine große Anzahl von Verfahren, mit denen teilweise sensible Daten verarbeitet werden, ohne ausreichende Datenschutzkonzepte und nicht bewertbare technische und organisatorische Maßnahmen im Echtbetrieb sind.

### 5.6 Datenerhebung bei Einbürgerungsverfahren

In diesem Jahr erreichte uns eine Beschwerde darüber, dass die Ausländerbehörde im Verfahren einer Ermessenseinbürgerung von den Antragsstellenden die Vorlage des aktuellen Arbeitsvertrages verlangte. Zwar sind in Einbürgerungsverfahren Nachweise darüber zu erbringen, dass die Antragstellerin beziehungsweise der Antragsteller imstande ist, sich und ihre beziehungsweise seine Angehörigen zu ernähren. Durch die Anforderung der Vorlage des Arbeitsvertrages werden aber auch Daten durch die Ausländerbehörde erhoben, die für die Bewertung des Antrags nicht erforderlich sind, wie zum Beispiel Arbeitszeiten oder etwaige Sonderregelungen. Nach entsprechendem Hinweis wurde uns von der Ausländerbehörde zugesichert, dass künftig lediglich gefordert würde, dass die Antragsstellerin beziehungsweise der Antragssteller eine Bestätigung des Arbeitgebers mit Angabe des Namens der Antragstellerin beziehungsweise des Antragstellers sowie Angaben über die Lohnhöhe und die Dauer des Arbeitsverhältnisses einreicht. Gegebenenfalls würde zudem die Erhebung von Angaben zur Berufsbezeichnung sowie zur Dauer einer gegebenenfalls vereinbarten, noch andauernden Probezeit erforderlich sein. Alternativ würde bei Bedarf von der Ausländerbehörde darauf hingewiesen, dass die Antragsstellerin beziehungsweise der Antragssteller Schwärzungen der nicht benötigten Angaben im Arbeitsvertrag vornehmen kann.

### 5.7 Datenschutzkonzepte bei der Polizei Bremen

Die Fachverfahren der Polizei Bremen verweisen bezüglich einiger zentraler Anforderungen an die Kontrollziele nach dem Bremischen Datenschutzgesetz auf das Rahmendatenschutzkonzept der Polizei Bremen. Zu diesem übergreifenden Konzept hatten wir bereits im letzten Jahr Stellung genommen und auf offene Fragen hingewiesen. Trotz der Bedeutung dieses Konzeptes für die datenschutzrechtliche und datentechnische Gesamtbewertung der einzelnen Fachverfahren der Polizei Bremen haben wir in diesem Jahr keine Antworten auf die noch offenen Fragen erhalten.

Darüber hinaus stellen wir auch bei der Beratung zu Fachverfahren fest, dass noch einige Antworten ausstehen. Dies betrifft beispielweise die Verschriftung von Telekommunikationsüberwachungsmaßnahmen in PIER (Polizeiliche Information Ermittlung Recherche), die Haft-Entlassenen-Auskunfts-Datei-Sexualstraftäter HEADS, die Einsatzleitzentrale der Polizei Bremen FELIS (Flexibles Einsatzleitsystem Innere Sicherheit) sowie die Vorabkontrolle diverser Anwendungen aus Intrapol (Intranetportal der Polizei).

Begründet wurde die fehlende Beantwortung der offenen Fragen seitens der Polizei Bremen mit Unklarheiten bezüglich der Zuständigkeit, internen Umstrukturierungen sowie mit zeitlichen Engpässen.

Aufgrund der Sensibilität der Daten, die bei der Polizei Bremen verarbeitet werden und die wir in der Regel mit dem Schutzbedarf hoch und sehr hoch bewerten, halten wir es für dringend erforderlich, dass gerade für Fragen des technischen Datenschutzes, und hier insbesondere für das Rahmendatenschutzkonzept, und zentrale Fachverfahren der Polizei Bremen Bearbeiterinnen und Bearbeiter zur Verfügung stehen.

### 5.8 Videoaufzeichnung in Einsatzfahrzeugen der Ortspolizeibehörde Bremerhaven

In diesem Berichtsjahr haben wir uns mit der Videoaufzeichnung nach § 29 Absatz 5 Bremisches Polizeigesetz (BremPolG) befasst. Dieses Verfahren hat die Orts-

polizeibehörde Bremerhaven in Anlehnung an das Verfahren der Polizei Bremen (vergleiche 30. Jahresbericht, Ziffer 9.1) gestaltet.

Die Ortspolizeibehörde legte uns eine Verfahrensbeschreibung sowie eine entsprechende Dienstanweisung vor. Die Unterlagen regeln die Aufzeichnung von Videodaten in Einsatzfahrzeugen in Anhaltesituationen und Kontrollsituationen. Uns wurde weiterhin versichert, dass die mit Videoaufzeichnungstechnik ausgerüsteten Fahrzeuge mit einem geeigneten Aufkleber versehen worden sind, der auf die Möglichkeit der Videoaufzeichnung hinweist.

Nach den vorliegenden Dokumenten ist das Gerät zum Beschreiben der Speicherkarten fest im Fahrzeug installiert und verschlossen. Ein Zugriff auf die Speicherkarten im Fahrzeug ist nur einem begrenzten Personenkreis mit einem speziellen Schlüssel möglich. Die Speicherkarten können an zentraler Stelle über ein spezielles Lesegerät ausgelesen werden.

Wir befinden uns derzeit in der Beratung und erwarten noch ergänzende Unterlagen zur Vorgehensweise im Auswertungsfall.

### 5.9 Polizeiliche Fahndung in sozialen Netzwerken

Die polizeiliche Fahndung in sozialen Netzwerken wurde im letzten Jahr von Polizeibehörden in einzelnen anderen Bundesländern durchgeführt und unter Berufung darauf auch in Bremen thematisiert. Die Fraktion der Christlich Demokratischen Partei Deutschlands (CDU) forderte in einem Bürgerschaftsantrag ein Modellprojekt zur polizeilichen Fahndung mit facebook. Auf Einladung des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit nahmen wir hierzu Stellung.

Die Öffentlichkeitsfahndung im Internet und insbesondere in sozialen Netzwerken wie facebook greift in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener (Tatverdächtiger oder auch Zeugen) ein, als dies bei der Nutzung klassischer Medien der Fall ist. Die Daten können mit wenigem Aufwand verbreitet und kopiert werden. Eine Löschung ist quasi unmöglich. Auch aus diesen Gründen bestimmen die Richtlinien für das Strafverfahren und für das Bußgeldverfahren (RiStBV), Anlage B, dass die Nutzung des Internets für Fahndungsausschreibungen nur in Ausnahmefällen und unter strikter Beachtung des Verhältnismäßigkeitsgrundsatzes erfolgen soll. Außerdem sollen private Internetanbieter grundsätzlich nicht eingeschaltet werden. In sozialen Netzwerken wie facebook kommt die Problematik hinzu, dass veröffentlichte Daten außerhalb der Verfügungsgewalt der verantwortlichen Polizei gespeichert werden. Die Daten, die im Zusammenhang mit dem Aufruf von facebook-"Fanseiten" entstehen, sind auf Servern in den Vereinigten Staaten von Amerika und unterliegen damit dem dortigen Recht. So können die amerikanischen Sicherheitsbehörden die Herausgabe der Daten von facebook verlangen, ohne dass die verantwortliche Polizeibehörde hier in Deutschland davon Kenntnis erlangt oder sogar Einfluss darauf hätte. Nach den gegenwärtig von facebook für den Betrieb von „Fanseiten" festgelegten Rahmenbedingungen könnte die Polizei ihrer Verantwortung somit sowohl in rechtlicher als auch in tatsächlicher Hinsicht nicht nachkommen (siehe Ziffer 11.2 dieses Berichts). Auch die Einbindung der Fahndungsaufrufe über einen Link stellt keine datenschutzkonforme Lösung dar.

Der Ausschuss für Wissenschaft, Medien, Datenschutz und Informationsfreiheit beschloss, den Antrag zur facebook-Fahndung erneut aufzurufen und zu diskutieren, sobald ein Beschluss der Innenministerkonferenz zu diesem Thema vorliegt.

Auch die Innenministerkonferenz sowie die Justizministerkonferenz haben sich in diesem Jahr mit der Thematik beschäftigt. Hierzu hat die Innenministerkonferenz einen Arbeitskreis eingesetzt. Der Arbeitskreis erarbeitete einen Bericht, der die datenschutzrechtlichen Probleme sowie die von facebook nicht offen kommunizierten Techniken benennt. Leider wurde das Papier bisher nicht abschließend der Konferenz der Chefs der Staatskanzleien und Senatskanzleien (CdS) vorgelegt, die sich nun voraussichtlich erst im Frühjahr 2013 mit dem Bericht inhaltlich befassen werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben sich in einem Schreiben an die Innenministerkonferenz sowie die Justizministerkonferenz gewandt, um ihre Auffassung darzulegen, auf die Risiken hinzuweisen und die Anforderungen an eine datenschutzkonforme Öffentlichkeitsfahndung darzulegen.

In Bremen wurde der Bürgerschaftsantrag „facebook-Fahndung einführen" an die staatliche Deputation für Inneres und Sport überwiesen, in deren Sitzung Anfang

November 2012 der Senator für Inneres und Sport mündlich über den Zwischenstand berichtete. Danach haben die Polizeien Nutzungskonzepte erarbeitet, die der Deputation vorgelegt werden sollen. Aktuell würden aber die Entwicklungen bei der Senatorin für Finanzen abgewartet (siehe Ziffer 11.2 dieses Berichts).

Wir werden unsere Position verstärkt gegenüber den bremischen Polizeien sowie dem Senator für Inneres und Sport vertreten und auf eine datenschutzkonforme Lösung für Öffentlichkeitsfahndungen drängen.

### 5.10 Neues Vorgangsbearbeitungssystem bei der Polizei

Die Polizeien im Land Bremen planen seit längerem die Einführung des neuen Vorgangsbearbeitungssystems @rthus. Der Produktivbetrieb soll 2014 starten. Im Sommer dieses Jahres fand ein erstes Gespräch zu dem Vorhaben zwischen Vertretern der Polizei Bremen, der Ortspolizei Bremerhaven und unserer Dienststelle zur Projektvorstellung statt. Wir wiesen in dem Gespräch und in unserer Stellungnahme auf unsere allgemeinen datenschutzrechtlichen Anforderungen an das neue polizeiliche Vorgangsbearbeitungssystem wie die Grundsätze der Datenvermeidung und Datensparsamkeit hin und erklärten, dass eine umfassende revisionssichere Protokollierung sicherzustellen ist. Außerdem wiesen wir darauf hin, dass der Schutzbedarf der Daten, die in @rthus gespeichert werden sollen, mit „hoch“ anzunehmen ist und dementsprechende Maßnahmen zu ergreifen sind. Besondere Anforderungen haben wir auch an das Authentifizierungsverfahren gestellt und erwarten hier die Vorlage eines geeigneten Konzeptes. Verfahrensbeschreibung und Datenschutzkonzept liegen derzeit ebenfalls noch nicht vor. Wir werden die Einführung des Vorgangsbearbeitungssystems weiterhin begleiten und die Polizeien des Landes Bremen so bei der datenschutzkonformen Ausgestaltung des Systems unterstützen.

### 5.11 Telekommunikationsüberwachung durch die Polizeien

Für die Polizei Bremen wird die Telekommunikationsüberwachung (TKÜ) zukünftig in verschiedenen Kooperationsstufen mit dem Landeskriminalamt (LKA) Niedersachsen durchgeführt werden. Hierfür wurde das Projekt „Datenschutzkonzept für die Telekommunikationsüberwachung in verschiedenen Kooperationsstufen mit dem LKA Niedersachsen“ bei der Polizei Bremen installiert. Leider kam es in dem Projekt immer wieder zu zeitlichen Verzögerungen, die unter anderem daraus resultierten, dass uns zeitweise kein Ansprechpartner bei der Polizei Bremen zur Verfügung stand. Da die Kooperation gegebenenfalls auf weitere norddeutsche Bundesländer ausgeweitet werden soll, ist es besonders wichtig, in diesem Projekt die Grundlage für eine datenschutzkonforme Lösung zu schaffen. Wir haben gegenüber der Polizei Bremen frühzeitig darauf hingewiesen, dass die komplette Datenverarbeitung für die Telekommunikationsüberwachung sowie die entsprechenden Geschäftsprozesse zu beschreiben sind. Daher haben wir gefordert, dass die Polizei Bremen als verantwortliche Stelle uns vor Aufnahme der sogenannten Vollkooperation mit dem LKA Niedersachsen als Auftragnehmer eine umfassende Dokumentation vorlegt. Dazu gehören unter anderem die Schutzbedarfsfeststellung, die Risikoanalyse, der Vertrag zur Datenverarbeitung im Auftrag nach § 9 Bremisches Datenschutzgesetz, die Beschreibung der getroffenen technischen und organisatorischen Maßnahmen, das IT-Sicherheitskonzept des Auftragnehmers, das Betriebskonzept des Auftragnehmers, die Verfahrensbeschreibung aller Systeme zur Aufzeichnung und Verarbeitung der Überwachungsmaßnahmen sowie die dazugehörigen Berechtigungskonzepte und Administrationskonzepte, die Fachkonzeption, die Beschreibung der Verschriftung der Gesprächsinhalte sowie die Beschreibung der sicheren Übertragung der Daten und der dafür eingesetzten zertifizierten Komponenten. Wenn Daten für mehrere Länder verarbeitet werden, ist insbesondere das Trennungsgebot zu beachten. Insofern ist eine detaillierte Beschreibung der Maßnahmen zum Trennungsgebot (hinsichtlich der Trennung der niedersächsischen personenbezogenen Daten und der bremischen personenbezogenen Daten einerseits und der einzelnen bremischen TKÜ-Verfahren andererseits) und der damit in Zusammenhang stehenden Gewährleistung der Mandantenfähigkeit des Systems erforderlich.

Zu den uns bisher eingereichten Unterlagen haben wir im Dezember des Berichtsjahres gegenüber der Polizei Bremen sehr umfassend Stellung genommen und einen umfangreichen Anforderungskatalog vorgelegt. Unseres Erachtens ist der Entwicklungsstand des Projekts derzeit noch nicht so weit fortgeschritten, dass den da-

tenschutzrechtlichen Anforderungen bezüglich der technischen und organisatorischen Anforderungen schon genüge getan wäre.

### 5.12 Fußballspielberechtigungen ausländischer Minderjähriger

Eltern minderjähriger ausländischer Spielerinnen und Spieler müssen bei Bremer Fußballvereinen ihre Arbeitsverträge, Arbeitserlaubnisse und Nachweise über die Nationalität einreichen. Der Bremer Fußballverband erklärte uns, dies sei zur Erstregistrierung auch im Amateurbereich nach dem FIFA-Reglement (deutsch: Internationale Förderation des Verbandsfußballs – Weltfußballverband) erforderlich. Begründet wurde dies mit dem Schutz Minderjähriger, der auch zu beachten sei, wenn ein internationaler Transfer nicht stattfinde. Diese Regelung gilt auch im Amateurbereich.

Dass die Vorlage dieser Dokumente für den Schutz Minderjähriger auch bei einer Erstregistrierung im Amateurbereich bei den Vereinen erforderlich ist, ist nicht nachvollziehbar. Wir halten die Vorlage dieser Dokumente im Amateurbereich weder für geeignet, Minderjährige zu schützen, noch für erforderlich und somit nicht für zulässig. Sie verstößt gegen das Bundesdatenschutzgesetz.

Zudem birgt die Klausel eine Benachteiligung minderjähriger ausländischer Spielerinnen und Spieler sowohl nach dem Grundgesetz als auch nach dem Allgemeinen Gleichbehandlungsgesetz. Der Bremer Fußballverband erklärte uns, im Falle einer Anordnung unserer Behörde, die Anforderung dieser Unterlagen zu untersagen, müsste den Betroffenen in Bremen das Spielrecht verweigert werden. Dies hätte zur Folge, dass minderjährige Spielerinnen und Spieler, die keine deutsche Staatsangehörigkeit haben und deren Eltern die Dokumente nicht vorlegen, in keinem Verein in Bremen Fußball spielen können.

Da das FIFA-Reglement in allen Verbänden in Deutschland und anderen Ländern gleichlautend anzuwenden ist, streben wir eine zumindest bundeseinheitliche Klärung an. Wir wollen über den Deutschen Fußballbund bei der FIFA darauf hinwirken, dass die Vorlage der Dokumente nur bei einem internationalen Transfer gefordert wird. Die Rückmeldungen der anderen Aufsichtsbehörden hierzu sind sehr ermutigend.

## 6. Justiz

### 6.1 Einführung eines Forderungsmanagements in der Justizverwaltung

Das Projekt „Forderungsmanagement in der Justiz“ wird gemeinsam von der Senatorin für Finanzen und dem Senator für Justiz und Verfassung durchgeführt. Ziel des Projekts ist die Wiederaufnahme von unbefristet niedergeschlagenen Forderungen und ihre erneute Geltendmachung sowie die Überprüfung von Möglichkeiten zur Effektivitätssteigerung bei der Beitreibung von Justizforderungen bei allen an dem Beitreibungsprozess beteiligten Dienststellen. Die Übertragung des Inkassowesens an Private wird dabei ausgeschlossen. Hintergrund des Projekts ist die Tatsache, dass in der bremischen Justiz jährlich Forderungen aus dem Haushaltstitel „Gerichtsgebühren und Geldstrafen“ in Höhe von etwa 1,3 Millionen Euro wegen Uneinbringbarkeit niedergeschlagen werden. Da sich die Lebensumstände der Schuldnerinnen und Schuldner im Laufe der Zeit ändern können, besteht die Chance, zu einem späteren Zeitpunkt nicht unerhebliche Forderungen realisieren zu können. Im Rahmen eines ersten Termins wiesen wir auf allgemeine datenschutzrechtliche Anforderungen hin, die bei dem Verfahren berücksichtigt werden müssen. Insbesondere ist ein Datenschutzkonzept zu erstellen und es muss eine Vorabkontrolle erfolgen. Datenerhebungen und Datenverarbeitungen dürfen nur dann erfolgen, wenn dafür eine Rechtsgrundlage besteht. Die elektronische Übermittlung personenbezogener Daten darf nur verschlüsselt erfolgen, ihr Transport in Papierform muss besonders gesichert sein. Zudem sind die datenschutzrechtlichen Grundsätze, beispielsweise die der Zweckbindung und der Erforderlichkeit zu beachten.

Inzwischen wurde uns ein Datenschutzkonzept für das Projekt zur Verfügung gestellt. Bevor eine abschließende Bewertung durch uns erfolgen kann, müssen jedoch noch einige offene Fragen geklärt werden. So bestehen beispielsweise noch Unklarheiten bezüglich der Rechtsgrundlagen, der Löschfristen und der technischen und organisatorischen Maßnahmen.

## 6.2 Videoüberwachung in der Justizvollzugsanstalt

Im Rahmen des Projekts „Sanierung der Justizvollzugsanstalt Bremen“ soll im Innenbereich und Außenbereich der Justizvollzugsanstalt Oslebshausen eine Videoüberwachung eingeführt werden. Zu Beginn des Jahres 2012 besichtigten wir die Baulichkeiten, um uns ein Bild über die geplante Installation der Überwachungskameras im Außenbereich zu machen. Davon umfasst werden sowohl das Anstaltsgelände als auch die direkte Umgebung der Anstalt. Die Beobachtung des letztgenannten Bereichs wird vom Senator für Justiz und Verfassung als notwendig angesehen, um sogenannte Mauerüberwürfe zu verhindern, mittels derer die Inhaftierten von außerhalb etwa mit Drogen oder auch Handys versorgt werden. Rauschmittel werden dazu beispielsweise in toten Vögeln oder Gegenständen wie Tennisbällen und Bauschutt versteckt und dann über die Anstaltsmauer auf das Innengelände geworfen. Es besteht daher vonseiten der Anstaltsleitung der Wunsch, auch die an die Anstalt angrenzenden Bereiche zu überwachen, um die „Mauerwerfer“ später überführen zu können. Wir wiesen darauf hin, dass keinesfalls in die Fenster der angrenzenden Häuser gefilmt werden dürfe. Eine Videoüberwachung darf nur in den Bereichen stattfinden, für die eine Rechtsgrundlage existiert. Zudem müssen rechtliche Voraussetzungen im jeweiligen Einzelfall vorliegen. Rechtsgrundlagen für eine Überwachung des Außenbereichs existieren bisher nur für die öffentlich zugängliche unmittelbare Anstaltsumgebung sowie im Bereich der Untersuchungshaft. In Zusammenarbeit mit einigen anderen Bundesländern ist ein Gesetz in Arbeit, um weitere Rechtsgrundlagen zu schaffen, das bisher aber noch nicht in Kraft getreten ist. Besonderer Aufmerksamkeit bedürfen in diesem Zusammenhang auch die Belange der Mitarbeiterinnen und Mitarbeiter der Justizvollzugsanstalt, die bei einer Videoüberwachung zwangsläufig mitgefilmt werden. Keinesfalls dürfen die Aufnahmen genutzt werden, um Bewegungsprofile von ihnen zu erstellen.

Hinsichtlich der Überwachung des Innenbereichs nahmen wir im Sommer des Berichtsjahres an einem Beratungstermin mit dem Personalrat der Justizvollzugsanstalt teil, der einige Fragen zu der Überwachung dieses Bereichs hatte.

Da das geplante Gesetz nicht verabschiedet werden wird, bevor die Videoanlage der Justizvollzugsanstalt fertig gestellt ist, sollen die Kameras für einen Übergangszeitraum nach der geltenden Rechtslage betrieben werden. Da von der Überwachung auch das Personal der Justizvollzugsanstalt betroffen ist, wurde uns der Entwurf einer Dienstvereinbarung übersandt. Wir wiesen den Senator für Justiz und Verfassung ausdrücklich darauf hin, dass eine Dienstvereinbarung fehlende Rechtsgrundlagen nicht ersetzen, sondern nur eine erlaubte Überwachung näher ausgestalten kann. Zudem legten wir noch einmal dar, in welchen Bereichen wir nach der aktuellen Gesetzeslage eine Überwachung für zulässig halten. Auch zu der Dienstvereinbarung nahmen wir Stellung. Insbesondere haben wir auf die Rechtsprechung des Bundesarbeitsgerichts zur Videoüberwachung der Beschäftigten hingewiesen. Danach erzeugt eine lückenlose Überwachung der Beschäftigten einen unzumutbaren Überwachungsdruck und wäre deshalb unzulässig.

Wir werden weiterhin die Einführung der Videoanlage sowohl im Innenbereich als auch im Außenbereich der Justizvollzugsanstalt begleiten.

## 6.3 Trojanereinsatz zur Telekommunikationsüberwachung

Aus der Presse hatten wir erfahren, dass angeblich im Jahr 2007 in Bremen durch das Landeskriminalamt (LKA) sogenannte Trojaner-Software zur Telekommunikationsüberwachung eingesetzt worden sei. Wir haben uns daraufhin mit dem LKA in Verbindung gesetzt um nähere Kenntnisse über den Vorgang zu gewinnen. Unsere Gespräche darüber waren zum Redaktionsschluss noch nicht abgeschlossen.

Im Rahmen der Fragestunde in der 7. Plenarsitzung der Bremischen Bürgerschaft (Landtag) vom 9. November 2011 hat der Innensenator berichtet, dass er davon ausgehe, dass Bremen zukünftig im Verbund mit Niedersachsen Quellen-Telekommunikationsüberwachung durchführen werde (siehe Ziffer 5.11 dieses Berichts). Am 13. September 2012 hat die Bremische Bürgerschaft (Landtag) den Senat aufgefordert, bis zur Einsetzung bundeseinheitlicher Software

— anzustreben, dass bei zukünftigen Beschaffungen von Software, die für Ermittlungszwecke beziehungsweise bei Überwachungen eingesetzt wird, den Behörden der Quelltext zur Verfügung gestellt wird,

— zu prüfen, ob bei bereits eingesetzter Überwachungssoftware nachträglich der Quelltext angefordert werden kann und

— sicherzustellen, dass Software, die für Ermittlungszwecke beziehungsweise Überwachungen eingesetzt wird, keine weiteren Funktionen beinhalten.

## 7. Gesundheit und Soziales

### 7.1 Versenden des Pflegekindergeldbescheides an die leiblichen Eltern

Im Januar des Berichtsjahres teilte uns eine Lehrerin einer Förderschule in Bremerhaven mit, dass sie im Rahmen einer Kurzzeitpflege spontan drei Schüler bei sich aufgenommen hatte. In dieser Angelegenheit hatte sie vom Amt für Jugend, Familie und Frauen (Jugendamt) Bremerhaven einen Bescheid über Pflegekindergeldleistungen erhalten, die ihr aufgrund dessen zustanden. In diesem Schreiben befand sich ein Hinweis, dass sie das Kindergeld, das ihr für die fünf Tage zustand, von der Mutter der drei Kinder erhalten würde und dass diese eine Zweitschrift des Bescheides erhalten habe. Auf Nachfrage, auf welchem Wege sie das Kindergeld erhalten könne, teilte ihr das Jugendamt mit, dass sie sich mit der Mutter der Pflegekinder in Verbindung setzen und ihr ihre Kontoverbindung mitteilen solle, damit diese ihr das Geld überweisen könne. Die Betroffene wandte ein, dass sie nicht damit einverstanden sei, woraufhin ihr vom Jugendamt mitgeteilt wurde, dass sie sich dann eben mit der Mutter treffen müsse, damit diese ihr das Geld persönlich übergeben könne. Dies sei das übliche Verfahren in solchen Fällen. Durch das Versenden der Zweitschrift an die Mutter der Pflegekinder hatte auch diese von der Höhe des Pflegekindergeldes erfahren, das die Betroffene aufgrund der Pflegschaft erhielt. Dies hatte zur Folge, dass die Kinder glaubten, die Lehrerin hätte die Kurzzeitpflege nur angenommen, um sich finanziell zu bereichern. Das Verhältnis zwischen der Lehrerin und den Schülern war seitdem stark belastet. Außerdem war durch dieses Vorgehen des Jugendamtes den Eltern die Adresse der Lehrerin bekannt geworden, obwohl das Jugendamt der Lehrerin zuvor aus Sicherheitsgründen von der Bekanntgabe ihrer Adresse gegenüber den Eltern der Pflegekinder abgeraten hatte.

Wir baten das Amt für Jugend, Familie und Frauen unter Hinweis auf die gesetzliche Übermittlungsregelung im Sozialgesetzbuch um Stellungnahme. Von dort wurde mitgeteilt, dass die Kindesmutter auf die Festsetzung eines Kostenbeitrages in Höhe des Kindergeldbetrages hingewiesen worden sei. Üblicherweise werde bei einer solchen Festsetzung eine Durchschrift des Pflegekindergeldbescheides ohne Adressfeld mitversendet, um die genaue Übersicht über diesen Betrag zu gewähren. Im Rahmen der Heranziehung zu den Kosten der Jugendhilfemaßnahmen sei es erforderlich, den kostenbeitragspflichtigen Personen die Gewährung der Leistung und ihre Verpflichtung zum Kostenbeitrag und die damit verbundenen Folgen für eine zivilrechtliche Unterhaltsverpflichtung mitzuteilen. Diese Mitteilung enthalte Angaben über Art und Umfang der Maßnahme sowie die Höhe der Leistungen und werde bei Einleitung einer Hilfemaßnahme immer an die Elternteile versandt. Leider sei in diesem Fall versäumt worden, das Adressfeld zu entfernen, sodass der Wohnort bekannt geworden sei. Im Rahmen einer Notaufnahme sei es eigentlich die übliche Praxis, nicht den Aufenthaltsort der Kinder mitzuteilen, um eine sichere Unterbringung zu gewährleisten. Es sei nicht zutreffend, dass üblicherweise den Pflegeeltern auferlegt wird, das ihnen für die Pflegezeit zustehende Kindergeld von den leiblichen Eltern einzutreiben. Für die Fehler wurde um Entschuldigung gebeten.

Wir teilten dem Amt für Jugend, Familie und Frauen daraufhin mit, dass wir auch die Versendung einer Durchschrift des Pflegekindergeldbescheids ohne Adressfeld an die leiblichen Eltern für unzulässig halten. Zum einen handelt es sich nicht um anonymisierte Daten, da die Identität der Pflegeeltern, sollte sie den leiblichen Eltern nicht sowieso bekannt sein, jedenfalls durch spätere Rückfrage bei den Kindern leicht herausgefunden werden kann. Durch die Übermittlung wird den leiblichen Eltern die Höhe des gegenüber den Pflegeeltern festgesetzten Pflegekindergeldes einschließlich des Grundbetrages (Mietanteil und Bekleidungsanteil, Kosten der Erziehung) bekannt. Dies ist zur Aufgabenerfüllung nicht erforderlich. Erforderlich ist lediglich die Information der leiblichen Eltern über den Anteil des Kindergeldes, der von ihnen eingezogen werden soll. Wir haben das Amt für Jugend, Familie und Frauen daher aufgefordert, zukünftig keine Durchschriften von Pflegekindergeldbescheiden mehr an die kostenpflichtigen Eltern zu versenden.

### 7.2 Bescheinigung des Sozialamtes für die GEZ

Im Mai des Berichtsjahres wandte sich ein Bürger an uns, der beim Amt für Soziale Dienste (Sozialamt) eine Bescheinigung zur Vorlage bei der Gebühreneinzugszentrale (GEZ) erbeten hatte, um für seinen Antrag auf Befreiung von der Rundfunkgebührenpflicht nachzuweisen, um welchen Betrag sein Einkommen den Sozialhilfebedarf übersteigt. Von Seiten des Sozialzentrums war ihm dafür eine vollständige Bedarfsberechnung übersandt worden, die neben der Information, um welchen Betrag das Einkommen den Sozialhilfebedarf übersteigt, eine Vielzahl sensibler Daten in Bezug auf die Höhe der Kosten der Unterkunft und sein Einkommen enthielt. Diese Sozialdaten waren für die GEZ zur Entscheidung über den Antrag auf Befreiung von der Rundfunkgebührenpflicht nicht erforderlich.

Der § 6 Absatz 2 des Rundfunkgebührenstaatsvertrags sieht vor, dass der Antragsteller die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht durch Vorlage einer Bestätigung des Leistungsträgers oder des Bescheides nachzuweisen hat. Die gesetzliche Regelung eröffnet damit verschiedene Möglichkeiten zum Nachweis der Berechtigung, von denen die datenschutzfreundlichste die Vorlage einer Bestätigung des Leistungsträgers ist, die lediglich die Information enthält, um welchen Betrag das Einkommen den Sozialhilfebedarf übersteigt.

Wir wandten uns daher an das Amt für Soziale Dienste und baten darum, dem Betroffenen eine solche Bescheinigung auszuhändigen und für diese Fälle ein Musterformular zu erstellen, das regelmäßig verwendet werden kann. Die Anregung hat das Amt für Soziale Dienste umgesetzt. Bereits Ende August 2012 konnten die Musterformulare an die Sozialzentren ausgegeben werden.

### 7.3 Bremer Rahmenvereinbarung zum Schutz von Kindern drogenabhängiger und substituierter Eltern

Im November 2011 erhielten wir von der Senatorin für Soziales, Kinder, Jugend und Frauen den Entwurf einer Kooperationsvereinbarung zum Schutz von Kindern drogenabhängiger und substituierter Eltern. Als Kooperationspartner waren darin die Senatorin für Soziales, Kinder, Jugend und Frauen, die Senatorin für Bildung, Wissenschaft und Gesundheit, das Amt für Soziale Dienste, das Gesundheitsamt Bremen, die Kassenärztliche Vereinigung Bremen, verschiedene Kliniken in Bremen, die Ärztekammer Bremen, der Berufsverband der Gynäkologinnen und Gynäkologen, der Berufsverband der Kinderärzte und Jugendärzte Landesverband Bremen sowie zwei Drogenhilfeeinrichtungen in privater Trägerschaft vorgesehen. Inhalt der Kooperationsvereinbarung war die verbindliche Vereinbarung einer Zusammenarbeit der Kooperationspartner im Umgang mit Kindern drogenabhängiger und substituierter Eltern sowohl im konkreten Einzelfall als auch einzelfallübergreifend. Dafür sollte unter anderem ein für alle Kooperationspartner verbindliches Meldeverfahren festgelegt werden.

Aus datenschutzrechtlicher Sicht hatten wir daran im Dezember 2011 aus verschiedenen Gründen Bedenken angemeldet. Zum einen fehlte es an einer konkreten Zweckbestimmung im Hinblick auf das Meldeverfahren. Es war nicht im Einzelnen festgelegt, welche Stelle welche Informationen an welche andere Stelle weitergeben soll und was mit einer Datenübermittlung im konkreten Einzelfall erreicht werden soll. Allein den Aufbau von umfassenden Datensammlungen bei allen unterzeichnenden Kooperationspartnern zu den betroffenen Personen hielten wir weder für geeignet noch für erforderlich, um die Sicherung des Kindeswohls zu erreichen.

Zudem wiesen wir darauf hin, dass die durch die unterzeichnenden Kooperationspartner vertretenen Berufsgruppen überwiegend einem besonderen Berufsgeheimnis oder Amtsgeheimnis unterliegen und daher nicht zu einer Datenübermittlung verpflichtet werden können. Sie haben im konkreten Einzelfall jeweils sorgfältig abzuwägen, ob vor dem Hintergrund der Gefahr der Zerstörung der Vertrauensbeziehung zur Patientin oder zum Patienten beziehungsweise zur Klientin oder zum Klienten und einem daraus im schlimmsten Fall resultierenden Abbruch der Beziehung die Weitergabe der in der jeweiligen Beziehung anvertrauten Information zu verantworten ist. Denn ein Abbruch der Hilfebeziehung könnte unter Umständen ebenfalls eine Gefahr für das Kindeswohl darstellen. Dabei sind auch die unterschiedlichen Rollen der einzelnen Berufsgruppen mit ihren jeweils eigenen Aufgaben zu beachten, die, soweit ihnen vertragliche Beziehungen mit den Betroffenen zugrunde liegen, nur mit deren Mitwirkung erweitert werden können. Für alle

Berufsgruppen gilt, dass die Erhebung, Nutzung, Speicherung und Übermittlung von personenbezogenen Daten jeweils nur zulässig ist, soweit es im konkreten Einzelfall zur Aufgabenerfüllung erforderlich ist und eine Rechtsvorschrift dies erlaubt oder die Einwilligung der Betroffenen vorliegt. Die Prinzipien der Vertraulichkeit, der Erforderlichkeit und der Zweckbindung sind für den Erfolg der Aufgabenerfüllung der jeweiligen Stellen wesentlich und sollten, auch bei Vorliegen einer Einwilligungserklärung und Schweigepflichtentbindungserklärung der Betroffenen, Beachtung finden. Zudem sollten etwaige Datenübermittlungen den Betroffenen gegenüber transparent gemacht werden, um die Vertrauensbeziehung nicht zu gefährden.

Von uns kritisiert wurde zudem, dass auch bei Verweigerung der Abgabe einer Schweigepflichtentbindungserklärung eine Datenübermittlung erfolgen sollte. Anders als dies der Entwurf der Vereinbarung voraussetzt, kann nicht davon ausgegangen werden, dass in diesen Fällen regelmäßig ein Fall des rechtfertigenden Notstandes nach § 34 Strafgesetzbuch (StGB) gegeben ist. Für eine Rechtfertigung nach § 34 StGB hätte der Berufsgeheimnisträger die Gefährdungssituation anhand der Umstände des Einzelfalls zu prüfen, eine Güterabwägung der widerstreitenden Interessen vorzunehmen und zu dem Ergebnis zu kommen, dass eine entsprechende Meldung geeignet und das mildeste Mittel ist, um die Gefahr abzuwenden. Die Meldung muss im konkreten Fall auch ein angemessenes Mittel sein. Im Regelfall wird es aber wohl bereits an einer konkreten Gefahrensituation für das Kind fehlen. Folge der Verweigerung muss daher in der Regel ein Verzicht auf die Datenübermittlung sein.

Problematisch sahen wir ebenfalls die Regelungen einer regelmäßigen Information der Kooperationspartner durch das Jugendamt und gemeinsamer Fallkonferenzen aller Kooperationspartner.

Ferner regten wir an, der Kooperationsvereinbarung Muster für die jeweils erforderlichen Einwilligungserklärungen beizufügen.

Weiter wiesen wir auf das zum 1. Januar 2012 in Kraft getretende Gesetz zur Kooperation und Information im Kinderschutz (KKG) hin, das eine Regelung zur Beratung und Übermittlung von Informationen durch Geheimnisträger bei Kindeswohlgefährdung trifft und empfahlen, die Kooperationsvereinbarung grundlegend anhand dieser Regelung zu überarbeiten.

Im Mai 2012 übersandte die Senatorin für Soziales, Kinder, Jugend und Frauen einen überarbeiteten Entwurf mit der Bezeichnung Bremer Rahmenvereinbarung zum Schutz von Kindern drogenabhängiger und substituierter Mütter/Väter/Eltern, der sich an der Regelung des KKG orientierte und in dem die wesentlichen unserer Kritikpunkte berücksichtigt waren. Im Anschluss daran erarbeiteten wir mit der senatorischen Behörde weitere Änderungen und Ergänzungen an dem Entwurf und halfen bei der Formulierung der Formulare für die Schweigepflichtentbindungserklärungen, sodass im September des Berichtsjahres alle unsere Bedenken ausgeräumt werden konnten. Die Rahmenvereinbarung konnte jedoch bis Ende des Berichtsjahres nicht in Kraft treten, da die Vertreter des Berufsverbandes der Kinder und Jugendlichen eine Unterzeichnung ablehnten, weil von dort ein weitergehender Datenaustausch gefordert wird.

### 7.4 Änderung des Bremer Krebsregistergesetzes

Im Juli 2010 erhielten wir vom Gesundheitsressort erstmalig einen Arbeitsentwurf zur Änderung des Bremer Krebsregistergesetzes (BremKRG). Im September 2011 wurde uns dann ein komplett überarbeiteter Änderungsentwurf übersandt, der in vielen Punkten eine wesentliche Verschlechterung des Datenschutzniveaus beinhaltete. Im Laufe des Berichtsjahres konnten wir gemeinsam mit dem Gesundheitsressort zwar einige datenschutzrechtliche Verbesserungen in dem Entwurf erreichen. Jedoch konnten bisher nicht alle unsere Bedenken ausgeräumt werden.

Erreichen konnten wir neben zahlreichen Konkretisierungen im Gesetzestext die Festschreibung technischer Anforderungen im Hinblick auf die Datensicherheit. Ebenso konnten wir durchsetzen, dass bei Vorliegen eines Widerspruchs der oder des Betroffenen gegen die Datenübermittlung an das Krebsregister weiterhin auf die Übermittlung von Diagnosedaten verzichtet wird. Zudem wird eine bestehende Regelung geändert, die die Übermittlung aller Todesbescheinigungen an die Vertrauensstelle des Krebsregisters erlaubt. Zukünftig sollen nur noch die für die Ver-

trauensstelle zur Aufgabenerfüllung erforderlichen Daten vom Mortalitätsindex übermittelt werden dürfen. Der Bremer Mortalitätsindex ist eine elektronische Datenbank, in der der komplette Inhalt aller Todesbescheinigungen von Verstorbenen mit erstem Wohnsitz im Bundesland Bremen erfasst wird. Verhindern konnten wir, dass zukünftig die Krankenversichertennummer, die einen lebenslang einheitlichen Teil zur Identifizierung der oder des Versicherten enthält, mit den Identitätsdaten der Versicherten in der Vertrauensstelle gespeichert wird. Es ist verfassungsrechtlich bedenklich, wenn ein lebenslang gleichbleibendes Kennzeichen in verschiedenen Zusammenhängen als Ordnungskennzeichen verwendet wird, ohne dass dies zwingend erforderlich ist. Zudem wird auf unsere Intervention hin auch weiterhin auf die Speicherung des Datums der ersten Tumordiagnose in der Registerstelle verzichtet; stattdessen wird weiterhin nur Monat und Jahr der ersten Tumordiagnose gespeichert. Ferner konnten wir erreichen, dass davon Abstand genommen wurde, eine Regelung zu schaffen, die es der Vertrauensstelle erlaubt, die Registerstelle bei der Durchführung wissenschaftlicher Forschung zu unterstützen. Mit einer solchen Regelung wäre die klare Trennung der Aufgaben der Vertrauensstelle und der Registerstelle aufgehoben worden. Außerdem wurde auf unsere Initiative hin die Aufbewahrungsfrist der Identitätsdaten von 50 Jahren nach dem Tod der Betroffenen auf 30 Jahre verkürzt.

Mit zahlreichen weiteren datenschutzrechtlichen Forderungen konnten wir uns jedoch nicht durchsetzen. Erst im Rahmen der Beratungen wurde uns bekannt, dass die bisherige Praxis der Eröffnung der Widerspruchsmöglichkeit gegen geltende Bestimmungen des BremKRG verstößt. Gesetzlich vorgesehen ist, dass den Betroffenen vor der Meldung der Ärzte an das Krebsregister eine Möglichkeit zum Widerspruch eingeräumt wird und dass im Falle des Widerspruchs nur ein erheblich reduzierter Datensatz an die Vertrauensstelle gemeldet wird. Dies wurde jedoch bei der Meldung durch Pathologen nicht umgesetzt. Die Meldung der Pathologen erfolgt ohne vorherige Information der Betroffenen; ein späterer Widerspruch gegenüber der behandelnden Ärztin beziehungsweise dem behandelnden Arzt führt dann nur noch zur Löschung der bereits gemeldeten Daten in der Vertrauensstelle. Wir forderten, die Praxis an die gesetzlichen Anforderungen anzupassen. Stattdessen wurde jedoch die bestehende Praxis im Änderungsentwurf legitimiert. Zudem forderten wir, dass in den Fällen, in denen die Betroffenen aus gesundheitlichen Gründen selbst nicht über ihre Krebserkrankung informiert werden, auf eine Meldung an das Krebsregister verzichtet wird oder dass in solchen Fällen wenigstens nur die Daten an das Krebsregister übermittelt werden, die auch im Fall eines Widerspruchs übermittelt werden dürfen. Das wurde vom Gesundheitsressort jedoch abgelehnt. Ebenfalls abgelehnt wurde die Streichung der Möglichkeit zur Übermittlung von Arztbriefen an das Krebsregister im geltenden BremKRG. Wir hatten diesbezüglich angeführt, dass es zumutbar und verhältnismäßig ist, dass unter Verwendung des dafür zur Verfügung gestellten Formblattes nur die zur Aufgabenerfüllung erforderlichen Daten an das Krebsregister übermittelt werden. Des Weiteren haben wir erhebliche Bedenken gegen eine Speicherung von Angaben zum Wohnsitz in der Registerstelle erhoben, die im Gesetz bereits erlaubt ist. Das Gesetz verlangt zwar, dass aufgrund der gespeicherten Angaben die Anschrift des Betroffenen nicht feststellbar ist. Dieser Anforderung genügt die aktuelle Praxis der Speicherung von Gauß-Krüger-Koordinaten jedoch nicht. Ferner haben wir uns vehement dagegen ausgesprochen, die Trennung zwischen Vertrauensstelle und Registerstelle des Krebsregisters aufzuweichen, indem der Vertrauensstelle zum Zweck der Zuordnung der Meldungen ein Zugriff auf die Datenbank der Registerstelle eingerichtet wird. Auch dies konnten wir jedoch nicht durchsetzen. Erhebliche Bedenken haben wir zudem gegen die Aufhebung der Beschränkung der Möglichkeit einer Datenübermittlung zu Forschungszwecken auf Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung erhoben. Wir haben uns deutlich gegen eine Datenübermittlung an Wirtschaftsunternehmen ausgesprochen, da die Gefahr des Missbrauchs der Daten zu wirtschaftlichen Zwecken, gegebenenfalls auch eine Reidentifizierung der Betroffenen durch das Hinzufügen von Zusatzwissen, aus unserer Sicht nicht ausgeschlossen werden kann. Wir forderten daher ein Festhalten an der Zweckbestimmung der unabhängigen wissenschaftlichen Forschung, konnten aber lediglich erreichen, dass die Daten nur an Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung übermittelt werden dürfen. Eine Verwendung der Daten zum Zweck unabhängiger wissenschaftlicher Forschung soll zukünftig keine Voraussetzung für eine Datenübermittlung an Dritte mehr sein, wenn das Vorhaben wissenschaftlichen Standards entspricht und ein berechtigtes, insbesondere wissenschaftliches, Interesse besteht. Zudem wandten wir

uns gegen die Änderungen, mit denen die in der Krebsfrüherkennungsrichtlinie des Gemeinsamen Bundesausschusses geregelte Evaluation der Mammographie umgesetzt werden soll. Wie wir bereits erfolglos vor Erlass der Richtlinie angeführt haben, birgt das dort geregelte Verfahren eine hohe potenzielle Gefahr der Zusammenführung von Identitätsdaten und Gesundheitsdaten und damit auch der Aufhebung der Anonymität der vom Krebsregister verwendeten Kontrollnummern. Zudem fehlt es an der Transparenz der Datenübermittlungen für die betroffenen Frauen. Wir kritisierten außerdem eine bestehende Regelung, die festlegt, dass die Vertrauensstelle und die Registerstelle sich an Qualitätssicherungsmaßnahmen, die sich im Rahmen der Zwecke nach § 1 BremKRG bewegen, beteiligen sollen. Diese Regelung ist nicht hinreichend bestimmt, da nicht festgelegt wird, welche Datenerhebungen, Datenverarbeitungen und Datennutzungen die Stellen dafür jeweils vornehmen dürfen. Wir halten daher eine Konkretisierung der Regelung für erforderlich, die jedoch nicht vorgenommen wurde.

Das Gesundheitsressort teilte uns mit, dass der Gesetzentwurf in Kürze in das förmliche Gesetzgebungsverfahren gehen wird.

### 7.5 Einziehung der Praxisgebühr durch Inkassodienstleister

Bereits im Juli 2011 meldete sich eine Bürgerin, die von einem Inkassodienstleister, einer Rechtsanwalts-GmbH aus Süddeutschland, aufgefordert worden war, die Praxisgebühr für ihre ärztliche Behandlung im Klinikum Bremen-Mitte zu überweisen. Der Inkassodienstleister teilte der Betroffenen mit, dass er die Kassenärztliche Vereinigung Bremen (KVHB) vertrete, die gesetzlich mit der Beitreibung der Praxisgebühr beauftragt sei und legte seinem Anschreiben eine Inkassovollmacht bei. Weiter wurde mitgeteilt, dass die Betroffene ihr aktuelles Forderungskonto im Internet unter Eingabe der dort genannten Zugangsdaten einsehen könne. Bei der Einsicht in das Onlineportal musste die Betroffene feststellen, dass unter ihren Zugangsdaten der Name einer anderen Person unter ihrer Anschrift gespeichert war. Die Nachfrage der Betroffenen, wie es dazu kommen konnte, wurde vom Inkassodienstleister und der KVHB nicht beantwortet. Im Onlineportal wurden für die Preisgabe der dort enthaltenen Informationen die Angabe von Telefonnummer und Faxnummer oder der E-Mail-Adresse verlangt. Da die Betroffene nicht bereit war, diese Daten anzugeben, wurde ihr die Einsicht im Portal verwehrt.

Auf Nachfrage teilte uns die KVHB mit, dass die Rechtsanwalts-GmbH bereits im Jahr 2007 mit Zustimmung der Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales mit dem Einzug der Praxisgebühr betraut worden sei. Die Rechtsanwalts-GmbH sei von der KVHB im Wege der Auftragsdatenverarbeitung nach § 80 Sozialgesetzbuch (SGB) X beauftragt worden und führe nur Hilfsdienste bei der Datenverarbeitung streng nach Weisung und ohne eigene Entscheidungsbefugnisse durch. Es würde lediglich ein Mahnschreiben mit dem von der KVHB vorgegebenem Inhalt versandt, gegebenenfalls eingehende Zahlungen verbucht und Einwendungen der Betroffenen entgegengenommen und ohne Bewertung an die KVHB weitergegeben. Zudem sei von der Rechtsanwalts-GmbH zur Verbesserung der Kommunikation und Information für die Betroffenen als zusätzliches freiwilliges Angebot ein Serviceportal eingerichtet worden.

Wir teilten der KVHB dazu mit, dass im vorliegenden Fall die Voraussetzungen für eine Datenverarbeitung im Auftrag nach dem Sozialgesetzbuch X nicht erfüllt waren. Im Fall der Leistungserbringung und Abrechnung im Rahmen von Gesamtverträgen haben die Kassenärztliche oder die Kassenzahnärztliche Vereinigung im Auftrag der Krankenkasse die Einziehung der Zuzahlung zu übernehmen, wenn die oder der Versicherte trotz einer gesonderten schriftlichen Aufforderung durch den Leistungserbringer nicht zahlt. Sie können hierzu Verwaltungsakte gegenüber den Versicherten erlassen. In den Bundesmantelverträgen kann ein abweichendes Verfahren vereinbart werden. Der Bundesmantelvertrag – Ärzte regelt, dass, wenn die beziehungsweise der Versicherte trotz einer schriftlichen Zahlungsaufforderung innerhalb der vom Arzt gesetzten Frist nicht leistet, die für den Arzt zuständige Kassenärztliche Vereinigung für den Vertragsarzt und die Krankenkasse den weiteren Zahlungseinzug übernimmt. Die Kassenärztliche Vereinigung führt hierzu ein Verwaltungsverfahren einschließlich Anhörung und Verwaltungsakt durch. Die Vollstreckung erfolgt in entsprechender Anwendung der Zivilprozessordnung. Demnach ist die Aufgabenerledigung durch die KVHB hier spezialgesetzlich eindeutig geregelt.

Die Voraussetzungen der Datenverarbeitung im Auftrag lagen hier nicht vor. Für eine solche wäre Voraussetzung, dass Sozialdaten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt werden. Die Anwendbarkeit der Regelung über die Auftragsdatenverarbeitung ist von der Übertragung der Aufgabenerfüllung (Funktionsübertragung) auf eine andere Stelle zu unterscheiden. Wesentliches Kriterium für eine Aufgabenübertragung und damit gegen das Vorliegen einer Auftragsdatenvereinbarung ist die Entscheidungsbefugnis der beauftragten Stelle über die Daten. Eine beauftragte Stelle kann immer nur datenverarbeitungsbezogene Hilfsfunktionen zur Erfüllung der Aufgabe des verantwortlichen Leistungsträgers leisten. Übernimmt die beauftragte Stelle auch die gesetzliche Aufgabe des Auftrag gebenden Leistungsträgers nach dem Sozialgesetzbuch, scheidet eine Datenverarbeitung im Auftrag aus. Nur in den Fällen, in denen die Aufgabe des Auftragnehmers in der bloßen Datenerhebung oder Datenverarbeitung ohne eigene Entscheidungsbefugnis liegt, ist eine Datenverarbeitung im Auftrag gegeben.

Im Hinblick auf die von der KVHB dargestellte Art und den Umfang der Beauftragung bestanden erhebliche Zweifel aufgrund der der Rechtsanwalts-GmbH erteilten Vollmachten, auf die sich diese gegenüber den Betroffenen berufen hatte. Mit einer Inkassovollmacht hatte die KVHB die Rechtsanwalts-GmbH zur außergerichtlichen Vertretung in allen Mahnsachen und Beitreibungssachen gemäß jeweils erteiltem Einzelmandat ermächtigt, die sich insbesondere auf die Vornahme und Entgegennahme von Zustellungen und den Empfang von Geldern erstreckt. Mit einer anderen Vollmacht ermächtigte die KVHB die GmbH mit der Erstellung außergerichtlicher Mahnschreiben, der Entgegennahme notwendiger Informationen, der Vornahme und Entgegennahme von Zustellungen, der Abgabe einseitiger Willenserklärungen, der Beseitigung des Streits über Bestand und/oder Umfang der Forderungen durch Vergleich, Verzicht, Anerkenntnis, der Entgegennahme von Geldern und Urkunden, der gerichtlichen Vertretung, der Rücknahme von Rechtsmitteln sowie dem Verzicht auf solche und der Zwangsvollstreckung, der Übertragung der Vollmacht ganz oder teilweise auf andere Berufsträger.

Es waren somit offenbar keine Verträge über eine Auftragsdatenverarbeitung abgeschlossen worden, sondern umfassende Vollmachten zur Übertragung der Aufgaben des Forderungseinzugs an die Rechtsanwalts-GmbH erteilt worden. Die Vollmachten enthielten die Übertragung von Aufgaben mit wesentlichen eigenen Entscheidungsbefugnissen der Beauftragten. Insbesondere die Befugnisse zur Abgabe von einseitigen Willenserklärungen, die Vornahme von Vergleichen, Entscheidungen über Verzicht und Anerkenntnis et cetera können nicht im Wege der Auftragsdatenverarbeitung an einer Auftragnehmerin oder einen Auftragnehmer übertragen werden. Zudem trat die Rechtsanwalts-GmbH in ihren Anschreiben gegenüber den Betroffenen als Vertreterin der KVHB auf und forderte diese auf, etwaige Rückfragen sowie sämtliche Korrespondenz ausschließlich über sie zu führen. Sie erscheint damit ihrem Gegenüber als verantwortliche Stelle. Dies widerspricht ebenfalls der gesetzlichen Regelung der Auftragsdatenverarbeitung, wonach die Rechte gegenüber dem Auftraggeber geltend zu machen sind. Zudem wurde von der Rechtsanwalts-GmbH im eigenen Namen ein Serviceportal im Internet zur Verfügung gestellt, in dem die Betroffenen ihr aktuelles Forderungskonto einsehen können. Auch dies war nicht mit der gesetzlichen Regelung vereinbar, wonach das Recht auf Auskunft gegenüber dem Auftraggeber geltend zu machen ist. Zudem stellt die Entscheidung über die Befriedigung eines Informationsbegehrens betreffend die zur Person gespeicherten Forderungsdaten ebenfalls keine Hilfstätigkeit dar.

Aus den genannten Gründen kann auf die hier vorgenommene Beauftragung der Rechtsanwalts-GmbH durch die KVHB die Regelung zur Auftragsdatenverarbeitung nicht angewendet werden. Aus den Vollmachten geht eindeutig hervor, dass die KVHB die gesamte gesetzliche Aufgabe des Forderungseinzugs einschließlich der außergerichtlichen und gerichtlichen Vertretung und etwaiger Zwangsvollstreckungsmaßnahmen an die Rechtsanwalts-GmbH übertragen hat. Diese Tätigkeiten gehen weit über Hilfstätigkeiten im Rahmen einer Auftragsdatenverarbeitung hinaus. Daher lag hier eine Aufgabenübertragung einschließlich der Übermittlung von Sozialdaten vor, die einer Rechtsgrundlage bedarf.

Da eine Rechtsgrundlage für die Übermittlung von Sozialdaten im konkreten Fall nicht ersichtlich war und auch die Voraussetzungen der Auftragsdatenverarbeitung nicht erfüllt waren, war die Übermittlung der Sozialdaten von der KVHB an die Rechtsanwalts-GmbH unzulässig. Daher haben wir die KVHB im Januar des Be-

richtsjahres aufgefordert, Art und Umfang der Beauftragung der Rechtsanwalts-GmbH den gesetzlichen Anforderungen entsprechend umzugestalten oder die Übermittlung von Sozialdaten an die Rechtsanwalts-GmbH unverzüglich zu beenden.

Im Februar des Berichtsjahres sagte die KVHB zu, die Verträge mit der Rechtsanwalts-GmbH zu ändern und uns zur Prüfung zu übersenden, da eine Beendigung der Zusammenarbeit nicht in Betracht käme. Nach wiederholter Nachfrage erhielten wir im Mai des Berichtsjahres ein Schreiben der KVHB, in dem diese darauf hinwies, dass entsprechende Konstellationen in zwei anderen Bundesländern nicht beanstandet worden seien. Die KVHB teilte weiter mit, dass sich der Umfang der Beauftragung der Rechtsanwalts-GmbH nicht aus den Vollmachten, sondern aus einem Mandatsvertrag ergebe. Die in der zweiten Vollmacht übertragenen Aufgaben würden durch die Rechtsanwalts-GmbH nicht ausgeführt. Diese würde für die KVHB nur im Stadium der vorgerichtlichen Mahnung tätig, ebenso wären Dienstleistungen im Zusammenhang mit dem rechtsförmlichen Verwaltungsverfahren, der Vertretung vor Sozialgerichten oder im Bereich der Zwangsvollstreckung vertraglich nicht vorgesehen und würden auch nicht durchgeführt. Die Mahnschreiben an die Versicherten seien geändert worden. Im Serviceportal würden keine personenbezogenen Daten der Versicherten mehr gespeichert.

Wir wiesen die KVHB darauf hin, dass für die Auftragsdatenverarbeitung die Erteilung eines schriftlichen Auftrags erforderlich sei. Der uns vorgelegte Mandatsvertrag genügte diesen Anforderungen jedoch nicht, darin fehlte die Beschreibung der zu treffenden technischen und organisatorischen Maßnahmen sowie Regelungen zu mitzuteilenden Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz von Sozialdaten oder gegen die im Auftrag getroffenen Festlegungen. Darüber hinaus war im Mandatsvertrag geregelt, dass durch die Rechtsanwalts-GmbH eine rechtliche Prüfung der Forderung erfolgt. Dies widersprach den Auskünften der KVHB, die uns gegenüber versichert hatte, dass von der Rechtsanwalts-GmbH lediglich Mahnschreiben versandt, Zahlungen verbucht und Einwendungen der Betroffenen entgegengenommen und ohne Bewertung an die KVHB weitergegeben würden. Zudem handelt es sich bei einer rechtlichen Prüfung nicht lediglich um eine Hilfstätigkeit bei der Erhebung, Verarbeitung oder Nutzung von Daten, sondern um Dienstleistung mit einer eigenen Entscheidungsbefugnis. Da diese Tätigkeit deshalb nicht im Wege der Auftragsdatenverarbeitung übertragen werden kann, bestand auch insoweit Änderungsbedarf am Mandatsvertrag. Weiter forderten wir die KVHB auf, beide Vollmachten zu widerrufen und zukünftig nicht mehr zu verwenden, da die darin geregelten Aufgaben, wie die außergerichtliche Vertretung in allen Mahnsachen und Beitreibungssachen gemäß jeweils erteiltem Einzelmandat, nicht im Wege der Auftragsdatenverarbeitung übertragen werden können. Ebenso waren auch die geänderten Mahnschreiben für die Empfänger weiterhin irreführend. Es wurde weiter der Briefkopf der Rechtsanwalts-GmbH verwendet und darauf hingewiesen, dass diese in Vertretung der KVHB handelt. Dies sollte jedoch nach den Ausführungen der KVHB gerade nicht zutreffend sein, die uns gegenüber darauf besteht, dass es sich hier nicht um anwaltliche Vertretung, sondern um Datenverarbeitung im Auftrag handele. Den Empfängern wurde jedoch weiter suggeriert, dass ein Anwaltsbüro mit der Durchsetzung der Forderung beauftragt worden ist.

Nach wiederholten Nachfragen erhielten wir Ende Oktober von der KVHB marginal geänderte Unterlagen sowie eine Vereinbarung zum Sozialdatenschutz zugesandt mit dem Hinweis, dass diese nunmehr zeitnah vom Vorstand unterzeichnet würden. Mit den Änderungen wurden die datenschutzrechtlichen Forderungen noch immer nicht umgesetzt. Stattdessen mussten wir durch Einsicht in das von der Rechtsanwalts-GmbH zur Verfügung gestellte Serviceportal feststellen, dass die Auskünfte der KVHB dazu wahrheitswidrig waren. Es war keineswegs so, dass in dem Portal keine personenbezogenen Daten der Betroffenen verarbeitet würden. Tatsächlich können sich die Betroffenen in dem Portal mit den im Anschreiben der Rechtsanwalts-GmbH genannten Zugangsdaten anmelden und durch Auswahl verschiedener möglicher Einwendungen durch das Portal prüfen lassen, ob die Praxisgebühr gezahlt werden muss. Nach Beantwortung der in diesem Zusammenhang im Portal gestellten Fragen, die sehr sensible Daten zur Gesundheit und sozialen Situation betreffen, wird den Betroffenen mitgeteilt, ob die Praxisgebühr bezahlt werden muss oder nicht. Soweit nach den Angaben der oder des Betroffenen eine Befreiung von der Praxisgebühr besteht, wird dazu aufgefordert, entsprechende

Nachweise zu übersenden oder hochzuladen und damit direkt an „die zuständigen Sachbearbeiter“ zu übermitteln. Soweit aufgrund der Angaben der oder des Betroffenen eine eindeutige Feststellung der Zahlungspflicht nicht möglich ist, stellt das Portal eine Maske für eine E-Mail der beziehungsweise des Betroffenen bereit, in dem dieser der Rechtsanwalts-GmbH den Sachverhalt schildern soll. Es wird versichert, dass die Rechtsanwalts-GmbH kurzfristig über diese Adresse mit den Betroffenen Kontakt aufnimmt und sich schnellstmöglich um Abhilfe bemüht. Entgegen der Behauptungen der KVHB erhebt und verarbeitet die Rechtsanwalts-GmbH daher Sozialdaten der Betroffenen mit Hilfe des im eigenen Namen betriebenen Serviceportals. Den Betroffenen wird mitgeteilt, dass die Einwendungen von der Rechtsanwalts-GmbH auch inhaltlich bearbeitet würden, was ebenfalls den Auskünften der KVHB widerspricht. Schriftliche Unterlagen über die Beauftragung der Rechtsanwalts-GmbH haben wir nicht erhalten.

Die KVHB hat damit ihre Pflicht zur Auskunft gegenüber der Landesbeauftragten für den Datenschutz aus dem Bremischen Datenschutzgesetz verletzt. Wir haben daher die Senatorin für Bildung, Wissenschaft und Gesundheit als zuständige Aufsichtsbehörde und Bußgeldbehörde für die KVHB informiert und um aufsichtsbehördliche Maßnahmen und die Prüfung der Einleitung eines Bußgeldverfahrens gebeten.

### 7.6 Datenerhebung durch Krankenkassen bei Verdacht auf Behandlungsfehler

Im März des Berichtsjahres wandte sich die Ärztekammer Bremen an uns und bat um datenschutzrechtliche Bewertung der Datenerhebung einer Krankenkasse beim behandelnden Arzt gegen den Willen einer Versicherten zum Zweck der Aufdeckung von eventuellen Behandlungsfehlern. Die Krankenkasse schrieb die Versicherte an und lud sie unter Hinweis auf einen möglichen Fehler bei einer ärztlichen Behandlung zu einem Beratungsgespräch ein. Die Versicherte, die mit der Behandlung zufrieden war, nahm den Termin nicht wahr. Daraufhin erhielt sie ein Schreiben von der Krankenkasse, in dem diese um eine Erklärung zur Entbindung von der Schweigepflicht bat, damit ein Sachverständigengutachten angefertigt werden könne. Nachdem der behandelnde Arzt in Absprache mit der Patientin der Krankenkasse deutlich gemacht hatte, dass die Patientin keine Schweigepflichtentbindungserklärung abgeben wolle, teilte die Krankenkasse dieser mit, dass sie diesen Wunsch respektiere und den Vorgang nunmehr abschließe. Acht Monate später erhielt die Versicherte von demselben Sachbearbeiter der Krankenkasse erneut eine Aufforderung, die Entbindung von der Schweigepflicht zu erklären und der Herausgabe der Patientenunterlagen zuzustimmen. Die Akten sollten an die Krankenkasse herausgegeben werden, die diese dann ihrerseits an den Medizinischen Dienst der Krankenversicherung (Medizinischer Dienst) weiterleiten wollte.

Das Vorgehen der Krankenkasse ist in diesem Fall datenschutzrechtlich wie folgt zu bewerten:

Krankenkassen dürfen Sozialdaten für Zwecke der Krankenversicherung erheben und speichern, soweit diese für die Unterstützung der Versicherten bei Behandlungsfehlern erforderlich sind. Die Krankenkassen können die Versicherten bei der Verfolgung von Schadensersatzansprüchen, die bei der Inanspruchnahme von Versicherungsleistungen aus Behandlungsfehlern entstanden sind und nicht auf die Krankenkassen übergehen, unterstützen. Diese Voraussetzungen lagen in diesem Fall jedoch nicht vor, da von der betroffenen Versicherten kein Behandlungsfehler geltend gemacht und daher auch keine Ansprüche aus einem Behandlungsfehler erhoben wurden. Die Unterstützung durch die Krankenkasse muss aber der Verfolgung von privatrechtlichen Schadensersatzansprüchen aus Vertrag oder unerlaubter Handlung dienen. Die gesetzlichen Voraussetzungen lagen demnach also nicht vor.

Nach dem Sozialgesetzbuch V dürfen die Krankenkassen Sozialdaten für Zwecke der Krankenversicherung auch erheben und speichern, soweit diese für die Beteiligung des Medizinischen Dienstes erforderlich sind. Dazu können die Krankenkassen in geeigneten Fällen durch den Medizinischen Dienst prüfen lassen, ob Versicherten bei der Inanspruchnahme von Versicherungsleistungen aus Behandlungsfehlern ein Schaden entstanden ist. Da hier jedoch die gesetzlichen Voraussetzungen, wie oben ausgeführt, nicht vorlagen, schied eine Einschaltung des Medizinischen Dienstes nach dieser Vorschrift aus. Jedoch kam eine Beauftragung des Medizinischen Dienstes nach einer anderen Vorschrift des Sozialgesetzbuches V

in Betracht, wonach die Krankenkassen in den gesetzlich bestimmten Fällen oder wenn es nach Art, Schwere, Dauer oder Häufigkeit der Erkrankung oder nach dem Krankheitsverlauf erforderlich ist, verpflichtet sind, bei Erbringung von Leistungen, insbesondere zur Prüfung von Voraussetzungen, Art und Umfang der Leistung, sowie bei Auffälligkeiten zur Prüfung der ordnungsgemäßen Abrechnung eine gutachtliche Stellungnahme des Medizinischen Dienstes der Krankenversicherung einzuholen. Darunter fällt auch die Begutachtung von unmittelbar im Zusammenhang mit Versicherungsleistungen stehenden Behandlungsfehlern. Fraglich ist aber, in welchem Umfang hier eine Datenerhebung und Datenspeicherung durch die Krankenkasse erforderlich war. Die Krankenkassen sind verpflichtet, dem Medizinischen Dienst die für die Beratung und Begutachtung erforderlichen Unterlagen vorzulegen und Auskünfte zu erteilen. Der Medizinische Dienst darf die für die Prüfungen, Beratungen und gutachtlichen Stellungnahmen erforderlichen Sozialdaten selbst erheben. Da er also die zur Wahrnehmung seiner Aufgaben erforderlichen Daten selbst erheben kann, ist eine entsprechende Datenerhebung und Datenspeicherung durch die Krankenkasse nicht erforderlich. Die Befugnis der Krankenkasse zur Erhebung und Speicherung von Sozialdaten betrifft daher nur die Daten, die erforderlich sind, um zu entscheiden, ob eine Beauftragung des Medizinischen Dienstes erfolgen soll. Ist diese Entscheidung bereits getroffen, sind die darüber hinaus für die Aufgabenerfüllung des Medizinischen Dienstes erforderlich Daten von diesem selbst zu erheben. Alternativ besteht die Möglichkeit, dass die Unterlagen von der Krankenkasse für den Medizinischen Dienst angefordert werden und dann direkt an den Medizinischen Dienst übermittelt oder der Krankenkasse in einem verschlossenen Umschlag zur Verfügung gestellt werden, den diese ungeöffnet an den Medizinischen Dienst weiterleitet.

Für die Datenerhebung durch den Medizinischen Dienst bedarf es jedoch nicht der Mitwirkung der Versicherten durch Erklärung einer Schweigepflichtentbindung der behandelnden Ärztin oder des behandelnden Arztes. Die Leistungserbringer sind in den Fällen, in denen die Krankenkassen eine gutachtliche Stellungnahme oder Prüfung durch den Medizinischen Dienst veranlasst haben, verpflichtet, Sozialdaten auf Anforderung des Medizinischen Dienstes unmittelbar an diesen zu übermitteln, soweit dies für die gutachtliche Stellungnahme und Prüfung erforderlich ist.

Ferner erlaubt das Sozialgesetzbuch V den Krankenkassen die Erhebung und Speicherung von Sozialdaten für Zwecke der Krankenversicherung, soweit diese für die Durchführung von Erstattungsansprüchen und Ersatzansprüchen erforderlich sind. Demnach könnte also eine Datenerhebungsbefugnis vorliegen, wenn Ansprüche übergegangen sind. In der Gesetzesbegründung zu dieser Regelung wird ausgeführt, dass Krankenkassen, wie andere Sozialversicherungsträger auch, die Aufgabe haben, im Falle der Schädigung ihrer Versicherten durch Dritte die dadurch bedingten Leistungsaufwendungen beim Dritten oder dessen Versicherung einzufordern. Dazu müssen ihnen die entsprechenden Daten zur Verfügung stehen. Hiermit wollte der Gesetzgeber sicherstellen, dass Krankenkassen die dazu erforderliche datenschutzrechtliche Grundlage bekommen (Bundestags-Drucksache 15/1525, Seite 142). Im konkreten Fall ist aber gar nicht ermittelt, ob tatsächlich ein Behandlungsfehler und somit eine Schädigung der Versicherten durch einen Dritten vorliegt. Die Krankenkasse sieht dafür offenbar Anhaltspunkte, die betroffene Versicherte nicht. Dabei ist zu beachten, dass die Durchführung der Ansprüche nicht erst deren tatsächliche Geltendmachung gegenüber Dritten erfasst, gegebenenfalls auf dem Rechtsweg, sondern auch bereits im Vorfeld die Prüfung, ob entsprechende Erstattungsansprüche oder Schadensersatzansprüche für die Krankenkasse entstanden sein könnten. Dies setzt aber sehr konkrete Hinweise auf haftungsrelevantes Verhalten voraus. Die Pauschalbehauptung, es läge ein Unfall vor, reicht dafür nicht aus (keine Verdachtserforschung). Um diese Prüfung durchführen zu können, ist die Krankenkasse aber berechtigt, Einsicht in Behandlungsunterlagen zum Zweck der Durchsetzung von Ansprüchen gegen Schadensersatzpflichtige beziehungsweise Erstattungspflichtige zu nehmen. Dies gilt insbesondere deswegen, weil die Krankenkasse im Bestreitensfall darlegungspflichtig und beweispflichtig ist, dass es sich um einen entsprechenden Erstattungsfall beziehungsweise Schadensersatzfall handelt. Welche Daten dabei von der Krankenkasse für die Prüfung, ob gegebenenfalls ein Behandlungsfehler vorliegt, konkret erhoben werden dürfen, orientiert sich am jeweiligen Einzelfall (Erforderlichkeit). Häufig wird bereits die Anforderung der sogenannten Epikrise, des Krankenhausentlassungsberichts, ausreichen.

Sind die oben genannten Voraussetzungen erfüllt, ist die Krankenkasse berechtigt, die Versicherten zur Mitwirkung aufzufordern, damit sie vom behandelnden Arzt die zur Geltung ihrer Schadensersatzansprüche erforderlichen Auskünfte erhält. Die Entbindung der behandelnden Ärzte von der Schweigepflicht durch den Versicherten stellt dabei eine Mitwirkungspflicht dar.

### 7.7 Verkauf von Rezeptdaten durch Apothekenrechenzentren

Nach Bekanntwerden der Praxis des Verkaufs von pseudonymisierten Rezeptdaten durch Apothekenrechenzentren haben wir uns im Berichtsjahr intensiv mit der Frage der Zulässigkeit der Übermittlung von Rezeptdaten durch Apothekenrechenzentren nach § 300 Absatz 2 Satz 2, 2. Halbsatz Sozialgesetzbuch V befasst. Der Prozess der Abstimmung eines datenschutzgerechten Verfahrens mit dem unserer datenschutzrechtlichen Aufsichtszuständigkeit unterliegenden Apothekenrechenzentrum konnte im Berichtsjahr noch nicht abgeschlossen werden.

### 7.8 Hausarztzentrierte Versorgung

Im November 2003 wurde in das Sozialgesetzbuch (SGB) V eine Regelung eingefügt, die die Hausarztzentrierte Versorgung (HzV) regelte. Später wurden die Hausärztinnen und Hausärzte dafür mit einem eigenständigen Verhandlungsmandat ausgestattet. Schließlich wurde im Januar 2009 in einer neuen gesetzlichen Regelung den Krankenkassen bis zum 30. Juni 2009 eine Frist gesetzt, um Verträge mit Gemeinschaften, die die Hälfte der an der hausärztlichen Versorgung teilnehmenden Allgemeinärztinnen und Allgemeinärzte vertreten, über eine HzV zu schließen. Anstelle der Abrechung über die Kassenärztliche Vereinigung (KV) sollte die Abrechnung über die Gemeinschaft erfolgen. Regelungen zur Verarbeitung von personenbezogenen Daten wurden jedoch nicht getroffen.

Ziel der sowohl für Versicherte als auch für die Hausärztinnen und Hausärzte freiwilligen HzV ist die Verbesserung der Qualität der hausärztlichen Versorgung durch Stärkung der zentralen Steuerungsfunktion und Koordinierungsfunktion der Hausärztinnen und Hausärzte. Der Vertrag kann von den Patientinnen und Patienten nach zwölf Monaten gekündigt werden; anderenfalls verlängert er sich um weitere zwölf Monate.

Vonseiten der Datenschutzaufsichtsbehörden wurde moniert, dass im Modell der HzV die Leistungen der Hausärztinnen und Hausärzte zwingend über private Rechenzentren abzurechnen waren, was datenschutzrechtlich nicht zulässig war. Damit dieses Modell nicht eingestellt werden musste, wurde im Juli 2009 vom Gesetzgeber eine Rechtsgrundlage für die Abrechnung über private Rechenzentren geschaffen, die zunächst befristet bis zum 30. Juni 2010 gelten sollte, im Juli 2010 jedoch noch um ein weiteres Jahr bis Ende Juni 2011 verlängert wurde.

Im Juli 2010 erließ das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) eine Verfügung gegen den Hausärzteverband Schleswig-Holstein, mit dem Inhalt, dass an die Auftragnehmer des Hausärzteverbandes keine Daten von Patientinnen und Patienten mehr übermittelt werden dürften und dass die bereits gespeicherten Daten durch den Hausärzteverband nicht genutzt werden dürften. Bemängelt wurde vom ULD, dass die Hausärztinnen und Hausärzte durch Nutzung einer vom Hausärzteverband vorgegebenen Software faktisch keine ausreichende Möglichkeit der Kontrolle über die Weitergabe von Patientendaten durch ihr Praxissystem mehr hätten. Zudem sah der Vertrag vor, dass sich die Ärztinnen und Ärzte verpflichtend eines bestimmten Auftragsdatenverarbeiters bedienen mussten, wenn sie von den für sie günstigen Hausarztabrechnungen Gebrauch machen wollten, obwohl sie weder rechtlich noch faktisch in der Lage waren, die Kontrolle über ihre Patientendaten als Auftraggeber wahrzunehmen. Der Hausärzteverband legte dagegen Widerspruch ein und beantragte einstweiligen Rechtsschutz beim Verwaltungsgericht Schleswig.

In Bremen wurde zwischen einigen Krankenkassen und dem Hausärzteverband Bremen keine Einigung über den Abschluss von Verträgen zur Umsetzung der HzV erzielt, sodass Schiedspersonen eingesetzt wurden, von denen die Vertragsentwürfe des Hausärzteverbandes dann in Schiedsverfahren in ihren wesentlichen Grundsätzen festgesetzt wurden. Dagegen wurde Klage beim Sozialgericht Bremen erhoben und einstweiliger Rechtsschutz beantragt.

Im August 2010 forderten wir den Hausärzteverband Bremen auf, bis zur gerichtlichen Entscheidung keine weiteren Verträge zur HzV in der bisher bekannten Form

abzuschließen und die abgeschlossenen Verträge vorläufig außer Kraft zu setzen. Dies wurde vom Hausärzteverband Bremen jedoch abgelehnt.

Ende September 2010 erging der Beschluss des Sozialgerichts Bremen im einstweiligen Rechtsschutzverfahren, in dem dieses die aufschiebende Wirkung der Klage gegen die Schiedsentscheidung zur Festsetzung eines HzV-Vertrages anordnete, da dieser voraussichtlich gegen Datenschutzrecht verstoße und damit offensichtlich rechtswidrig erscheine. Gegen diesen Beschluss wurde Beschwerde eingelegt.

Entsprechend entschied auch das Verwaltungsgericht in Schleswig Anfang Oktober 2010 im dort anhängigen einstweiligen Rechtsschutzverfahren. Dagegen wurde beim Oberverwaltungsgericht (OVG) in Schleswig Beschwerde eingelegt. Im Januar 2011 wurden vom OVG Schleswig-Holstein durch Beschluss im vorläufigen Rechtsschutzverfahren die datenschutzrechtlichen Bedenken bestätigt.

Vonseiten der Aufsichtsbehörden wurden fortlaufend Gespräche über eine datenschutzgerechte Umsetzung der Verträge über die HzV geführt. Dabei wurde insbesondere darauf hingewiesen, dass bei einer Auftragsdatenverarbeitung die Anforderungen von § 80 SGB V eingehalten werden müssen, was bei einem Modell mit einzelnen Hausärztinnen und Hausärzten als Auftraggeber wohl praktisch nicht möglich ist, und dass die eingesetzte Vertragssoftware überarbeitet werden muss. Eine Einigung mit den Hausärzteverbänden konnte jedoch nicht erzielt werden. Daher forderten wir vom Hausärzteverband Bremen nach dem Beschluss des OVG Schleswig-Holstein eine grundlegende Überarbeitung der vorgelegten Vertragsentwürfe.

Der Bundesgesetzgeber hat dann jedoch eine Erlaubnisnorm für die bisher unzulässige Datenverarbeitung geschaffen. Mit § 295 a SGB V wurde den Hausärztinnen und Hausärzten erlaubt, die Daten der Patientinnen und Patienten an die Hausärzteverbände als verantwortliche Stelle oder die von diesen beauftragten Rechenzentren zum Zweck der Abrechnung zu übermitteln.

In der Folge hob das Landessozialgericht Bremen-Niedersachen im November 2011 den Beschluss des Sozialgerichts Bremen auf und wies die Anträge auf einstweiligen Rechtsschutz ab. Hinsichtlich der datenschutzrechtlichen Regelungen im HzV-Vertrag, die nach Auffassung des Gerichts zum Teil gegen Datenschutzrecht verstießen, wurde den Vertragsparteien aufgegeben, diese im Hinblick auf die neue Rechtslage und die datenschutzrechtlichen Anforderungen anzupassen.

Der Hausärzteverband Bremen und einige betroffene Krankenkassen baten uns um eine datenschutzrechtliche Bewertung der von Ihnen überarbeiteten Vertragsentwürfe. Da uns eine vollumfängliche datenschutzrechtliche Prüfung der sehr umfangreichen Vertragsentwürfe aufgrund unserer engen personellen Kapazitäten nicht möglich war, baten wir die Krankenkassen und den Hausärzteverband Bremen um Benennung einzelner Fragestellungen, um dazu punktuell Stellung zu nehmen. Daraus ergaben sich für uns noch die folgenden Defizite: Für die in den Vertragsentwürfen vereinbarte Übermittlung der Teilnahmeerklärungen an das vom Hausärzteverband beauftragte Rechenzentrum zum Zweck der Einschreibung der Versicherten gibt es keine Rechtsgrundlage. § 295 a SGB V erlaubt lediglich die Datenübermittlung zu Abrechnungszwecken. Des Weiteren muss für die Teilnahme der Versicherten nach der Anpassung der Verträge und der Änderung der gesetzlichen Grundlagen eine neue Einwilligungserklärung eingeholt werden. In Bezug auf die vom Hausärzteverband vorgegebene Software, die wir aus Kapazitätsgründen nicht prüfen konnten, forderten wir, dass ein datenschutzrechtliches Niveau erreicht wird, das dem Sicherheitsstandard des KV-SafeNet entspricht (siehe dazu 33. Jahresbericht, Ziffer 4.4.2). Insbesondere sollte sichergestellt sein, dass das Prüfmodul, als im Rahmen eines Praxisinformationssytems bereitgestelltes Modul, unabhängig von der Systemebene jederzeit bei Bedarf während des laufenden Betriebs aktiviert und deaktiviert werden kann, dass es revisionsfähig ist, dass die vom Prüfmodul als Ergebnis gelieferten Daten jederzeit durch die Ärztin oder den Arzt im Einzelnen verifiziert werden können und dass die Aktivierung der Verschlüsselungsfunktion durch den Arzt nach inhaltlicher Prüfung vorgenommen werden kann.

Unseres Wissens sind die Verträge über die HzV im Berichtszeitraum nicht mehr in Kraft gesetzt worden.

### 7.9 Datenübermittlung durch Apotheken bei Ärztehopping von Substitutionspatienten

Die Apothekerkammer Bremen wandte sich an uns und berichtete, dass in Apotheken aufgefallen sei, dass Substitutionspatienten häufig viele verschiedene Ärz-

te aufsuchen, um sich unter Verschweigen ihres Substitutionshintergrundes bestimmte Arzneimittel verschreiben zu lassen. Durch Wechselwirkungen dieser Präparate bestehe ein hohes gesundheitliches Risiko, zum Teil sogar Lebensgefahr, für die Betroffenen. Um die Verschreibungen dieser Arzneimittel an Substitutionspatienten zu unterbinden, hielt es die Apothekerkammer für angezeigt, dass die Apotheken, in denen diese Fälle bekannt würden, die Kassenärztliche Vereinigung oder die Ärztekammer Bremen informieren, damit eine dieser Stellen die verschreibenden Ärzte informiert.

Aus datenschutzrechtlicher Sicht ergeben sich bei diesem Verfahren die folgenden Probleme:

Die Information der Kassenärztlichen Vereinigung beziehungsweise der Ärztekammer durch die Apotheke über ein entsprechendes Verschreibungsverhalten stellt eine Übermittlung von Gesundheitsdaten dar, die nur zulässig ist, soweit sie durch das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift erlaubt oder angeordnet ist oder in die die beziehungsweise der Betroffene eingewilligt hat. Eine datenschutzrechtliche Rechtsgrundlage gibt es nicht. Die Übermittlung der Daten aufgrund einer Einwilligungserklärung der Betroffenen kommt hier nicht in Betracht. Daher wäre diese Datenübermittlung unzulässig.

Es handelt sich hier um Gesundheitsdaten, die dem besonderen Berufsgeheimnis nach § 203 Strafgesetzbuch (StGB) unterliegen. Die Verletzung dieses Berufsgeheimnisses ist strafbewehrt. Das Vorliegen der Voraussetzungen des Rechtfertigenden Notstandes nach § 34 StGB könnte zwar eine Strafbarkeit ausschließen; diese Regelung kann aber nicht als subsidiäre Rechtsgrundlage für hoheitliche Eingriffe herangezogen werden. Zweifel bestehen im Übrigen auch bereits daran, ob die Voraussetzungen von § 34 StGB hier erfüllt sind, da zumindest die Einschaltung der Ärztekammer beziehungsweise der Kassenärztlichen Vereinigung jedenfalls nicht erforderlich sind, um die Gesundheitsgefahr im konkreten Fall abzuwenden. Eine Information der verschreibenden Ärzte ohne Zwischenschaltung einer weiteren Stelle wäre diesbezüglich ausreichend.

Hinzu kommt, dass – soweit eine Prüfung und Verfolgung von Fällen des Ärztehoppings durch die Ärztekammer oder die Kassenärztliche Vereinigung erfolgen soll – es dafür einer entsprechenden gesetzlichen Aufgabenzuweisungsnorm und gesetzlichen Rechtsgrundlagen der dafür erforderlichen Datenerhebungen, Datenverarbeitungen und Datennutzungen bedarf. Entsprechende gesetzliche Regelungen gibt es zurzeit nicht, sodass dies nach der aktuellen Rechtslage nicht zulässig ist.

### 7.10 Übersendung von Arztbriefen per Fax

Ein Klinikum in Bremen plante, bei der Entlassung der Patientinnen und Patienten Arztbriefe nicht wie bisher per Post, sondern per elektronischem Fax an die weiterbehandelnden Ärztinnen und Ärzte zu versenden. Es wurde darin gegenüber der herkömmlichen Übermittlung der Vorteil gesehen, dass die weiterbehandelnde Ärztin beziehungsweise der weiterbehandelnde Arzt den Brief bereits im Vorfeld des Eintreffens der zu Behandelnden zur Kenntnis nehmen könne. Wir wiesen das Klinikum auf die Vorschriften des Bremischen Datenschutzgesetzes hin, wonach die verantwortliche Stelle bei der elektronischen Übertragung oder während des Transports von personenbezogenen Daten zu gewährleisten hat, dass diese nicht unbefugt gelesen, verändert oder entfernt werden können. Medizinische Daten sind als besondere Arten von personenbezogenen Daten im Sinne des Bremischen Datenschutzgesetzes besonders schutzbedürftig. Bei ihrer Übermittlung ist somit ein besonders hoher Schutz erforderlich. Bei der Übersendung von medizinischen Daten per elektronischem Fax kann ein ausreichender Schutz nicht gewährleistet werden, weil beim Einsatz von herkömmlichen und elektronischen Faxgeräten die Gefahr des unbefugten Lesens eingegangener Faxsendungen auf Empfängerseite besteht; insbesondere dann, wenn die Geräte in frei zugänglichen Bereichen aufgestellt sind. Zudem könnten Unbefugte Kenntnis vom Inhalt vertraulicher Faxsendungen erlangen, wenn die Verteilung innerhalb der empfangenden Organisation fehlerhaft ist oder die Faxe durch Falscheingabe von Faxnummern oder die versehentliche Anwahl falscher Adressaten, beispielsweise aus Kurzwahllisten oder Adressbüchern heraus fehlgeleitet werden. In diesem Zusammenhang ist besonders das Risiko zu erwähnen, dass innerhalb von Adressbüchern von Faxgeräten die Möglichkeit besteht, Gruppen von Empfängern zusammenzufassen, was zur Folge

hat, dass die Faxe dann an alle Empfängerinnen und Empfänger dieser Gruppe versandt werden. Kritisch ist auch zu betrachten, dass Faxe empfängerseitig sehr oft in E-Mails umgewandelt werden und dann im E-Mail-Postfach der Adressatin oder des Adressaten auflaufen. Es ist dabei nicht auszuschließen, dass diese

E-Mails dann über das Internet beispielsweise an mobile Endgeräte weitergeleitet werden. Da die Anforderungen des Bremischen Datenschutzgesetzes bei der Übermittlung von Gesundheitsdaten per Fax nicht gewährleistet werden können, ist die Nutzung dieses Mediums nur in sehr eng begrenzten Ausnahmefällen, in denen eine besondere Eilbedürftigkeit besteht, zulässig. In diesen Fällen sind geeignete technische und organisatorische Sicherheitsmaßnahmen zu treffen.

### 7.11 Bericht aus dem Arbeitskreis Gesundheit und Soziales

Im Arbeitskreis Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurden im Berichtsjahr unter anderem die folgenden Themen behandelt: Ergebnismitteilungen und Befundmitteilungen des Medizinischen Dienstes der Krankenversicherungen (MDK), Erhebung medizinischer Daten durch die gesetzlichen Krankenkassen, zum Beispiel bei Arbeitsunfähigkeit, ohne unmittelbare Beteiligung des MDK, datenschutzrechtliche Überprüfung von Arztbewertungsportalen im Internet, Verträge zur hausarztzentrierten Versorgung, Datenerhebung, Datenverarbeitung und Datennutzung bei der Qualitätsprüfung nach § 299 Strafgesetzbuch V, Nutzung eines Scientific-Use-Files bei der kassenärztlichen Versorgung, Datenabgleichverfahren im Sozialrecht (Bundesausbildungsförderungsgesetz, Wohngeld, Unterhaltsvorschussgesetz), Begrüßungsbesuche bei Eltern Neugeborener, Beendigung des Elektronischen Entgeldnachweis (ELENA)-Verfahrens, Einforderung der Praxisgebühr durch eine von der Kassenärztlichen Vereinigung beauftragte Anwaltskanzlei, Ausgestaltung von Projekten der Integrierten Versorgung, privatärztliche Verrechnungsstellen, Datenerhebung einer Krankenkasse bei einem Krankenhaus auf vertraglicher Grundlage, Weitergabe von anonymisierten Rezeptdaten durch Apothekenrechenzentren, einrichtungsübergreifende elektronische Patientenakte, Entwurf eines Gesetzes zur Verbesserung der Rechte von Patientinnen und Patienten (Patientenrechtegesetz), Aufbewahrung von Patientenakten nach Insolvenz einer Reha-Klinik, Meldungen der Ärztekammern an das Substitutionsregister beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM), Fragebogen Blutspender und Plasmaspender, Nationale Kohorte (Netzwerk deutscher Forschungseinrichtungen), Deutscher Schmerzfragebogen, Verhältnis zwischen den gesetzlichen Krankenkassen und dem MDK, Fallsteuerung im Arbeitsunfähigkeitsmanagement – Krankengeldfallmanagement, Callcenter bei gesetzlichen Krankenkassen, Vorlage des Einkommensteuerbescheides zur Beitragsberechnung bei der gesetzlichen Krankenkasse, Erhebung von Wundprotokollen durch gesetzliche Krankenkassen/Pflegekassen bei Pflegeeinrichtungen, Entwurf eines Gesetzes zur Weiterentwicklung der Krebsfrüherkennung und zur Qualitätssicherung durch klinische Krebsregister, Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (E-Government-Gesetz), „Anvertraute“ Sozialdaten, Telearbeit und Sozialdatenschutz, Elektronische Patientenquittung der Krankenkasse, Datenschutz in Arztpraxen, Bedarfsermittlungsbögen der „Internationalen Fördergemeinschaft Kinder-Rehabilitation und Jugend-Rehabilitation e. V. (rehaKIND)“, Wechsel in der Arztpraxis.

## 8. Bildung, Wissenschaft und Kultur

### 8.1 Geplatzter Einsatz einer Überwachungssoftware in Schulrechnern

Im November 2011 wurden wir über den Gesamtvertrag zur Einräumung und Vergütung von Ansprüchen nach dem Urheberrechtsgesetz informiert. Der Vertrag wurde zwischen den Bundesländern und den Verwertungsgesellschaften für Schulbuchproduktionen und Musikproduktionen abgeschlossen. Er enthält eine Klausel, wonach sich die Länder verpflichten, mit einer von den Verlagen zur Verfügung gestellten Plagiatssoftware die Schulrechner zu überprüfen. Als Voraussetzung für den Einsatz wurde festgelegt, dass die Software datenschutzrechtlich unbedenklich sein müsse. Wir haben erhebliche Bedenken gegen deren Rechtmäßigkeit. Es dürfte außer Frage stehen, dass auf Schulcomputern regelmäßig eine Vielzahl personenbezogener Daten über Schülerinnen und Schüler sowie Lehrkräfte verarbeitet werden. Die Daten unterliegen dem Fernmeldegeheimnis und berühren das Recht

auf Vertraulichkeit und Integrität informationstechnischer Systeme, soweit die private Nutzung der Rechner und des Internets in den Schulen zumindest stillschweigend geduldet wird.

Auf unsere Anfrage hat die Senatorin für Bildung, Wissenschaft und Gesundheit erklärt, sie habe im Hinblick auf einzelne Klauseln rechtliche Bedenken geltend gemacht. Sie seien jedoch zugunsten eines zügigen Abschlusses des Vertrages zurückgestellt worden. Bei einem Scheitern des Vertrages wären die im Vertrag festgelegten kostenlosen Vervielfältigungen für den Unterrichtsgebrauch und Prüfungsgebrauch aus urheberrechtlich geschützten Werken nicht möglich gewesen. Des Weiteren ist uns zugesagt worden, dass im Land Bremen keine Software ohne Prüfung durch uns eingesetzt würde. Diese Zusage ist auch vom Senat in seiner Antwort vom 6. Dezember 2011 (Drucksache 18/155) auf eine Kleine Anfrage der Fraktion Bündnis 90/Die Grünen gegeben worden.

Gleichzeitig wurde in den Medien über die Überwachungssoftware sehr ausführlich berichtet und debattiert. Im Frühjahr 2012 hat das für die Bundesländer federführende Bayerische Staatsministerium für Unterricht und Kultur erklärt, die Länder und die Bildungsverlage seien sich einig, dass auf den Einsatz der Software verzichtet werde. Wir sind froh, dass der öffentliche Sturm der Entrüstung gegen diese maßlose Art von Überwachung die Vertragspartner zum Einlenken gebracht hat.

### 8.2 Keine Kommunikation zwischen Lehrkräften und Schülerinnen und Schülern in sozialen Netzwerken

Wir haben Hinweise erhalten, Schulen würden ihre Homepage mit sozialen Netzen durch sogenannte Social-Plugins, gemeint sind damit Erweiterungen für externe Seiten, die ein Teilen der Inhalte mit Gruppen in sozialen Netzwerken ermöglichen sollen, verknüpfen. Insoweit sind sie mitverantwortlich für die damit zusammenhängende Verarbeitung personenbezogener Nutzerdaten durch soziale Netzwerke, die ihren Sitz in den Vereinigten Staaten von Amerika (USA) haben, beispielsweise facebook, Google+ und Twitter. Nicht nur das Betätigen des „Gefällt-mir"-Knopfes bei facebook, sondern das bloße Aufrufen der Webseite löst eine Datenübermittlung in die USA und eine unübersichtliche Weiterverwendung der Daten durch facebook aus (zur datenschutzrechtlichen Bewertung des Netzwerkes facebook siehe 34. Jahresbericht, Ziffern 1.2.1, 1.2.2, 1.2.3, 12.5 und die Ziffer 11.2 dieses Berichts). Ebenso hätten Lehrkräfte ihre Schülerinnen und Schüler darauf hingewiesen, über facebook könnten sie weitere Informationen für den Unterricht erhalten oder sich für die Behandlung der Problematik mit sozialen Netzwerken im Unterricht ein Profil anlegen. Die damit zusammenhängende Verarbeitung personenbezogener Schülerdaten erfolgt ohne wirksame Einwilligung der Betroffenen. Zudem verstößt sie gegen das Bremische Schuldatenschutzgesetz, weil die Datenverarbeitung über unsichere soziale Netzwerke nicht für den Erziehungsauftrag und Bildungsauftrag der Schulen erforderlich ist. Wir haben die Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Datenschutz bei sozialen Netzwerken jetzt verwirklichen" vom 28. September 2011 an die Schulaufsichtsbehörden in Bremen und Bremerhaven zur Beachtung in den Schulen weitergeleitet.

Daraufhin hat die Senatorin für Bildung, Wissenschaft und Gesundheit eine Verfügung erlassen. Unter Verweis auf die vorgenannte Entschließung der Konferenz hat sie die Schulen aufgefordert, den datenschutzkonformen Umgang mit sozialen Netzwerken sicherzustellen. Außerdem wurden die Schulen aufgefordert, den „Gefällt-mir"-Knopf auf den eigenen Webseiten unverzüglich zu entfernen. Das Schulamt Bremerhaven hat erklärt, die betroffenen Schulen beziehungsweise Lehrkräfte seien veranlasst worden, die Plugins zu entfernen. Ansonsten hätten sämtliche Schulen in Bremerhaven dem Schulamt mitgeteilt, ihre Lehrkräfte würden die Schülerinnen und Schüler nicht zur Nutzung von facebook in der vorgenannten Weise veranlassen.

Inzwischen hat sich aus dem „Runden Tisch Digitale Kultur und Schule" eine kleine Arbeitsgruppe unter Federführung des Zentrums für Medien im Landesinstitut für Schule gebildet. Die Mitglieder der Arbeitsgruppe kommen aus dem Zentrum für Medien, dem Technologie-Zentrum Informatik und Informationstechnik der Universität Bremen, des Zentralelternbeirats und der Landesbeauftragten für Datenschutz und Informationsfreiheit. Die Arbeitsgruppe erarbeitet zur Unterstützung der Lehrkräfte eine Handreichung für soziale Netzwerke in den Schulen. Die Hand-

reichung soll die unzulässige Kommunikation der Lehrkräfte mit Schülerinnen und Schülern in unsicheren sozialen Netzwerken sowie die damit verbunden erheblichen Risiken für die Persönlichkeitsrechte verdeutlichen. Außerdem sollen Fallbeispiele das Bewusstsein stärken, dass auch vermeintlich sichere Privateinstellungen und deren regelmäßige Anpassung und Überprüfung keine sichere Kommunikation gewährleisten. Gerade bei facebook werden die Nutzungsbedingungen und Nutzungseinstellungen sehr häufig geändert, sodass es eines unzumutbaren Aufwands der Nutzerinnen und Nutzer bedarf, hier regelmäßig die gewünschten Nutzungseinstellungen wieder vorzunehmen.

### 8.3 Recherche über Schülerinnen und Schüler in sozialen Netzwerken

Die Senatorin für Bildung, Wissenschaft und Gesundheit schickte als Schulaufsichtsbehörde in der Stadt Bremen eine E-Mail an bestimmte Schulleitungen. Darin wurde über einen Streikaufruf von Schülerinnen und Schülern im sozialen Netzwerk facebook informiert. Dieser E-Mail war ein Anhang beigefügt, der einen Auszug einer facebook-Fanseite erhielt, aus dem sich viele Namen von Schülerinnen und Schülern und anderen Nutzerinnen und Nutzern ergaben, die sich an der Debatte über den Streikaufruf beteiligt hatten. Dadurch wurden personenbezogene Daten der Betroffenen durch die Schulaufsichtsbehörde erhoben, gespeichert und an die Schulleitungen übermittelt. Die Betroffenen hatten darüber keine Kenntnis. Wir haben die senatorische Behörde darauf hingewiesen, dass eine Befugnis zur Verarbeitung dieser Daten ohne Kenntnis der Betroffenen nicht besteht.

Die Behörde hat eingeräumt, es handele sich eindeutig um ein Vergehen gegen geltende Rechtsvorschriften. Anlass dieser Recherche im Internet sei hauptsächlich ein Hinweis auf einen öffentlichen Streikaufruf über facebook gewesen, um entsprechende Vorsorgemaßnahmen für diesen Streikaufruf zur Absicherung der Behörde und der Schulen treffen zu können.

Daraufhin haben wir die Schulaufsichtsbehörde unter Hinweis auf das Bremische Datenschutzgesetz gebeten, die unzulässig gespeicherten Daten zu löschen und die Schulleitungen zu veranlassen, den betreffenden Anhang der E-Mail zu löschen und sich dies bestätigen zu lassen. Dies gilt auch für eventuell erfolgte Ausdrucke, die zu vernichten waren. Die Senatorin für Bildung, Wissenschaft und Gesundheit hat uns daraufhin mitgeteilt, unsere vorgeschlagenen Maßnahmen seien umgesetzt worden.

### 8.4 Keine Weiterleitung sensibler Schülerdaten per unverschlüsselter E-Mail

Wir baten die Senatorin für Bildung, Wissenschaft und Gesundheit um Auskunft, ob die Schulen und die Schulaufsichtsbehörde sensible Schülerdaten unverschlüsselt per E-Mail weiterleiten. Des Weiteren fragten wir nach, welche alternativen technischen und organisatorischen Maßnahmen bei der elektronischen Übertragung von Schülerdaten sicherstellen, dass sie nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Sensible Schülerdaten sind beispielsweise Abiturgutachten, Noten sowie Gesundheitsgutachten.

Daraufhin teilte die senatorische Behörde mit, sie beabsichtige eine entsprechende Verfügung zu erlassen, die sie uns im Entwurf vorlegte. Darin ist die Verpflichtung enthalten, die im häuslichen PC der Lehrkraft oder Betreuungskraft gespeicherten Schülerdaten zu verschlüsseln. Hierzu sollte diesem Personenkreis aus unserer Sicht eine angemessene Software zur Verfügung gestellt werden.

Dies ist zwar ein Schritt in die richtige Richtung. Erkennbar ist jedoch nicht, ob diese Verschlüsselung auch für die Weiterleitung der Daten an andere Stellen verwendet werden soll oder kann. Dazu haben wir beim Ressort nachgefragt und ergänzend noch Folgendes vorgeschlagen: Wir halten es für notwendig, dass die Lehrkräfte und Betreuungskräfte für den Empfang und die Weiterleitung von Schülerdaten am häuslichen PC eine dienstliche E-Mail-Adresse erhalten und verwenden. Damit kann der unbefugte Zugriff auf Schülerdaten beim Datentransport erheblich besser verhindert werden. Außerdem ist die Speicherung von Schülerdaten auf separaten und nicht privaten E-Mail-Postfächern besser vor einem unbefugten Zugriff, beispielsweise durch Mitbewohnerinnen und Mitbewohner, geschützt. Dies ist besonders wichtig, wenn eine Lehrkraft oder Betreuungskraft und eine Mitbewohnerin oder ein Mitbewohner ein gemeinsames privates Benutzerkonto benutzen.

Die Senatorin für Bildung, Wissenschaft und Gesundheit hat inzwischen erklärt, durch neue technische Voraussetzungen könne nun die lange erwartete Verschlüsselung und Signatur von E-Mails über digitale Zertifikate erfolgen. Damit könne auch Kommunikation per E-Mail verschlüsselt werden. Zudem bestehe jetzt die Möglichkeit, alle Lehrkräfte mit einer dienstlichen E-Mail-Adresse auszustatten. Die Umsetzung soll nach Angaben der senatorischen Dienststelle bis Ende 2012 umgesetzt werden. Wir werden das Vorhaben begleiten und dabei darauf achten, dass die Vorgaben erfüllt werden.

### 8.5 Erhebung von Bankverbindungsdaten bei Einlösung eines Gutscheins zum Besuch einer Kulturveranstaltung

Im Berichtszeitraum wandte sich ein Bürger an uns und machte uns auf einen Sachverhalt aufmerksam, den er datenschutzrechtlich für bedenklich hielt. Beim Ausfüllen eines Online-Bestellformulars, das eine Kultureinrichtung zum Verkauf von Eintrittskarten bereitstellte, hatte er in einem hierfür vorgesehenen Textfeld angegeben, dass er einen Gutschein besäße. Wie verlangt, hatte er zugleich die Gutscheinnummer und den Gutscheinwert eingegeben. Der Gutscheinwert deckte vollständig den Preis der zur Abholung an der Abendkasse bestellten Eintrittskarten. Gleichwohl konnte der Kartenbesteller seine Bestellung im System nicht abschließen, ohne dass er noch zusätzlich die mit einem Stern als Pflichtangaben gekennzeichneten Textfelder zu seinen Bankverbindungsdaten ausfüllte.

Personenbezogene Angaben dürfen auch in einem Vertragsverhältnis nur insoweit erhoben werden, als sie zur Vertragsbegründung und Vertragsdurchführung benötigt werden. Erfolgt die Vertragsbegründung in einem Online-Verfahren, so muss dieses ebenfalls so ausgestaltet sein, dass nur die notwendigen Angaben beim Vertragspartner erfragt werden. Das Online-Bestellformular entsprach dieser datenschutzrechtlichen Vorgabe offenkundig nicht. Wird ein Gutschein mit einem Gutscheinwert eingelöst, der den Kartenpreis deckt, muss der Kartenpreis nicht mehr im Wege des Bankeinzugsverfahrens beglichen werden. Eine Kenntnis der Bankverbindungsdaten des Bestellers ist nicht erforderlich.

Weiterhin sah das Online-Bestellformular vor, dass Telefonnummer und E-Mail-Adresse der Kartenbesteller als Pflichtangaben anzugeben waren. Als Grund hierfür nannte uns die Kultureinrichtung insbesondere, dass man Besucher etwa über Veranstaltungsausfälle informieren müsse. Datenschutzrechtlich hielten wir die Erhebung dieser Angaben gleichwohl nicht für erforderlich, da es jeder Besucherin und jedem Besucher überlassen werden kann, ob sie oder er diese besondere Serviceleistung in Anspruch nehmen möchte. Entspricht dies ihren Wünschen, können sie auf freiwilliger Basis die insoweit erforderlichen Kontaktdaten hinterlassen.

Nach einigem Hin und Her zeigte sich die Kultureinrichtung schließlich einsichtig und änderte das Online-Bestellformular sowohl im Hinblick auf etwaige Gutscheineinlösungen als auch auf die Freiwilligkeit der Angabe von Telefonnummer und E-Mail-Adresse ab.

## 9. Umwelt, Bau und Verkehr

### 9.1 Aufbauseminare nach der Fahrerlaubnisverordnung

Eine Petentin, die Kursleiterin für besondere Aufbauseminare nach der Fahrerlaubnisverordnung ist, machte uns auf eine datenschutzrechtliche Problematik bei der Kontrolle der Kurse durch den Senator für Umwelt, Bau und Verkehr aufmerksam. Die Seminare dürfen nur von speziell anerkannten Fachkräften durchgeführt werden und richten sich an Teilnehmende, die Verkehrsdelikte unter Rauschmitteleinfluss begangen haben. Im Anerkennungsbescheid, den der Senator für Umwelt, Bau und Verkehr der Petentin erteilt hatte, war eine Klausel enthalten, wonach die Leiterinnen und Leiter der Seminare zum Zwecke der Aufsicht über die Kurse gestatten müssten, dass Vertretungspersonen der Anerkennungsbehörde an den Kursen ganz oder teilweise teilnehmen.

Die Petentin hielt diese Regelung für problematisch, da den Teilnehmenden die Zusicherung von Vertraulichkeit sehr wichtig sei. In den Seminaren sollten die Ursachen ergründet werden, die zu den Verkehrsdelikten geführt hätten. Dabei sei es notwendig, dass die Teilnehmenden sehr persönliche Hintergründe offenbarten. Die Bereitschaft dazu könne erheblich durch die Anwesenheit von Dritten in den Seminaren beeinträchtigt werden.

Wir teilten dem Senator für Umwelt, Bau und Verkehr mit, dass wir im Interesse der Sicherheit des Straßenverkehrs zwar die Notwendigkeit sehen, eine fachlich einwandfreie Durchführung der Seminare zu gewährleisten. Nach unserer Auffassung ist es daher auch grundsätzlich zulässig, dass Sachverständige zu Kontrollzwecken an den besonderen Aufbauseminaren teilnehmen. Allerdings darf der Eingriff in das Persönlichkeitsrecht der Betroffenen durch Maßnahmen der Qualitätssicherung nur in dem Maße stattfinden, wie er zur Erreichung des Kontrollzwecks unbedingt erforderlich ist. Aus diesem Grund halten wir es für erforderlich, dass den Teilnehmenden der Seminare entweder die Verwendung von Aliasnamen gestattet wird oder das Einverständnis aller Betroffenen hinsichtlich der Anwesenheit der kontrollierenden Person vorliegt. Zudem ist es notwendig, die Betroffenen zu Beginn des Seminars über den Zweck der Teilnahme der Kontrollperson zu informieren und klarzustellen, dass es ihr nicht um im Rahmen des Seminars behandelte personenbezogene Daten der Teilnehmerinnen und Teilnehmer geht. Des Weiteren muss das Kontrollpersonal zur Wahrung des Amtsgeheimnisses verpflichtet worden sein. Der Senator für Umwelt, Bau und Verkehr stimmte unseren Anforderungen zu.

### 9.2 Verfahrensmanagement Großraumtransporte und Schwertransporte

Der Senator für Umwelt, Bau und Verkehr leitete uns den Entwurf eines Staatsvertrages aller Bundesländer über das Zusammenwirken zum Betrieb, zur Einrichtung und zur technischen Weiterentwicklung des Systems Verfahrensmanagement Großraum- und Schwertransporte (VEMAGS) mit der Bitte um Kenntnisnahme und Stellungnahme zu. Das Verfahren soll dazu dienen, das Erlaubnisverfahren für Fahrzeuge, deren Abmessungen, Achslasten oder Gesamtgewichte die gesetzlich allgemein zugelassenen Grenzen überschreiten, zu unterstützen. Da das Thema alle Bundesländer betrifft, wurde es bereits im länderübergreifenden Arbeitskreis Verkehr der Datenschutzbeauftragten des Bundes und der Länder besprochen. Zwar werden in dem Verfahren in erster Linie Firmendaten und Fahrzeugdaten gespeichert, gleichwohl findet auch eine vereinzelte Erfassung von personenbezogenen Daten statt. Es kann nicht mit letzter Sicherheit ausgeschlossen werden, dass auch anhand der Fahrzeugdaten Rückschlüsse auf einzelne Fahrerinnen und Fahrer möglich sind. Insofern bedurfte der Staatsvertrag einer näheren datenschutzrechtlichen Prüfung. So hatten wir Anmerkungen zu verantwortlichen Stellen, zum juristischen Betreiber, zur Anwendbarkeit des Hessischen Datenschutzgesetzes nach dem Staatsvertrag und zur Speicherung von Protokolldaten, wobei es sich teilweise aber lediglich um Unklarheiten handelte. In welcher Endfassung der Vertrag abgeschlossen wird, bleibt abzuwarten. Nach unseren Informationen soll der Staatsvertrag im April 2013 in der Verkehrsministerkonferenz beraten und danach von den Länderparlamenten ratifiziert werden und etwa im September 2013 in Kraft treten.

### 9.3 Vergabe von Sperrmüllterminen

Wiederholt äußerten Bürgerinnen und Bürger uns gegenüber den Verdacht, es würden bei der Vergabe von Sperrmüllterminen personenbezogene Daten unbefugt an Dritte weitergeleitet werden. Der Verdacht beruhte darauf, dass häufig kurze Zeit nach Herausstellen der Gegenstände durch die Betroffenen organisierte Sperrmüllsammler Verwertbares einsammelten und mitnahmen. Es bestand die Vermutung, dass die Sperrmüllsammler unbefugt Kenntnis von den Abfuhrtagen und Adressen der Betroffenen erlangt hatten. Bei der Prüfung des Verfahrens zur Vergabe der Sperrmülltermine beim Senator für Umwelt, Bau und Verkehr konnten wir keine auffälligen Schwachstellen erkennen, die auf eine unbefugte Weitergabe von Daten schließen ließen. Dabei können vereinzelte unbefugte Datenübermittlungen naturgemäß nicht mit völliger Sicherheit ausgeschlossen werden. Im Rahmen der Prüfung wurde uns mitgeteilt, dass es sich bei den Sperrmüllsammlern in der Regel um Mitglieder sehr gut vernetzter Großfamilien handele, die auf Motorrädern systematisch die Straßen abführen, um so den Sperrmüll aufzufinden. Per Handy würden dann Fahrer von Lieferwagen informiert, die die Gegenstände einsammelten. Es werde aber geprüft, dass Sperrmüllsystem umzustellen.

### 9.4 Ausbau des Glasfasernetzes in Bremerhaven

Ein Telekommunikationsunternehmen plant an verschiedenen Standorten – darunter in einigen Stadtteilen Bremerhavens – den Ausbau des Glasfasernetzes zum Zwecke einer schnelleren Datenkommunikation. Um die Haushalte mit Glasfaser-

anschlüssen versorgen zu können, bedarf es der Heranführung der Glasfaserleitungen an das jeweilige Gebäude. Eine Verlegung der Glasfaserkabel ist nur mit Zustimmung der Grundstückseigentümerinnen und Grundstückseigentümer zulässig. Die Kosten für die Verlegung würde in diesem Fall das Unternehmen tragen. Voraussetzung dafür sei, dass genügend Interessentinnen und Interessenten für die mit dem Glasfasernetz verbundenen Produkte vorhanden seien, da andernfalls das Projekt unwirtschaftlich sei. Um die Betroffenen anschreiben zu können, strebte das Unternehmen eine Übermittlung der Eigentümerdaten aus dem Liegenschaftskataster an. Wir teilten daraufhin dem Unternehmen mit, dass wir eine entsprechende Übermittlung auf Grundlage des bremischen Vermessungs- und Katastergesetzes für unzulässig halten. Zulässig wäre lediglich – da die Förderung des Ausbaus des Glasfasernetzes zu den Aufgaben der öffentlichen Verwaltung im Bereich der Daseinsvorsorge gehört – eine Übermittlung der Daten an den Magistrat der Stadt Bremerhaven, der dann ein Informationsschreiben an die betroffenen Eigentümerinnen und Eigentümer versenden könnte. Interessierte Eigentümerinnen und Eigentümer müssten sich dann über eine Kontaktadresse an das Unternehmen wenden. Nur in diesen Fällen würde das Unternehmen, das an dem Erfolg dieser Lösung zweifelte, Kenntnis von den Eigentümerdaten erhalten. Zwar ist unter bestimmten Voraussetzungen eine Übermittlung von Daten aus dem Liegenschaftskataster auch an Private zulässig, allerdings bezieht sich diese Erlaubnis nur auf Einzelfälle. Das Telekommunikationsunternehmen wollte aber gerade die Übermittlung einer Vielzahl von Adressdaten, die das Gesetz nicht vorsieht. Für das Unternehmen besteht darüber hinaus die Möglichkeit, die Eigentümerdaten aus dem Grundbuch zu erhalten. Die Einsicht des Grundbuches ist nämlich allen gestattet, die ein berechtigtes Interesse darlegen. Nach Aussage des Unternehmens ist diese Datenquelle jedoch aus technischen Gründen nicht geeignet.

Nach unserem derzeitigen Kenntnisstand ist bisher keine Datenübermittlung aus dem Liegenschaftskataster an das Unternehmen erfolgt, sondern ein Bürgerinformationsschreiben vom Magistrat an die Betroffenen versendet worden. Zudem wurde zur Information interessierter Immobilienbesitzerinnen und Immobilienbesitzer eine Annonce in einer Tageszeitung veröffentlicht, was wir für eine datenschutzgerechte Lösung halten.

### 9.5 Ausnahmegenehmigungen zum Parken für Pflegedienste

Im Rahmen ihrer Tätigkeit können Mitarbeiterinnen und Mitarbeiter von Pflegediensten Ausnahmegenehmigungen für das Abstellen ihres Kraftfahrzeugs in kostenpflichtigen oder eingeschränkten Parkzonen beantragen. Hierfür forderte das Bürger- und Ordnungsamt Bremerhaven unter anderem den Arbeitsvertrag an, wenn es sich um eine Ausnahmegenehmigung für ein Privatfahrzeug handelt. Uns erreichte eine Beschwerde, in der zu Recht darauf hingewiesen wurde, dass im Arbeitsvertrag zahlreiche Informationen über das Arbeitsverhältnis enthalten sind, die für die Ausstellung der Ausnahmegenehmigung nicht erforderlich sind. Daher wirkten wir beim Bürger- und Ordnungsamt Bremerhaven sowie beim Amt für Straßen und Verkehr Bremen darauf hin, dass zukünftig lediglich eine Bescheinigung des Arbeitgebers mit den erforderlichen Angaben über das bestehende Arbeitsverhältnis angefordert wird.

## 10. Finanzen und Verwaltungsmodernisierung

### 10.1 Durchführung einer Telefonverkehrsmessung in der Verwaltung der Stadt Bremerhaven

Der Magistrat der Stadt Bremerhaven hatte beschlossen, eine Telefonverkehrsmessung zu beauftragen. Eine entsprechende von der Landesbeauftragten für Datenschutz und Informationsfreiheit begleitete Messung wurde bereits in Bremen zur Entwicklung des „Bürgertelefons Bremen“ durchgeführt. Zweck der Telefonmessung in Bremerhaven ist die Optimierung der Telefontechnik sowie der gesamten Telekommunikationsleistungen bei der Stadtverwaltung und den städtischen Einrichtungen. Zudem soll der Bürgerservice durch die Zusammenführung aller Telefonangelegenheiten mit einer zentralen Vermittlungsstelle verbessert werden. Zur Zeit ist die telefonische Erreichbarkeit bei der Stadtverwaltung heterogen organisiert; das bedeutet, dass die Erreichbarkeit über eine zentrale Rufnummer nicht gewährleistet ist. Bei der Telefonmessung sollen gruppenbezogen Telefonaufkommen, die Dauer der Gespräche sowie die Dauer bis zur Herstellung einer Verbindung

innerhalb der Stadtverwaltung ermittelt werden. Wichtig ist dabei aus datenschutzrechtlicher Sicht, dass die Auswertungen nicht einzelfallbezogen erfolgen, keine Gesprächsinhalte erfasst werden und kein Mitarbeiterbezug hergestellt werden kann. Im Zusammenhang mit der Prüfung der Verfahrensbeschreibung für die Verkehrsmessung wiesen wir unter anderem daraufhin, dass nach dem Bremischen Datenschutzgesetz vor der Entscheidung über die Einführung oder die wesentliche Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden sollen, durch den behördlichen Datenschutzbeauftragten eine Vorabkontrolle vorzunehmen ist. Da eine Auftragsdatenverarbeitung geplant ist, machten wir den Magistrat noch einmal ausdrücklich auf die entsprechenden datenschutzrechtlichen Vorschriften aufmerksam, wonach in einem schriftlichen Auftrag die Datenverarbeitung, die technischen und organisatorischen Maßnahmen sowie etwaige Unterauftragsverhältnisse festzulegen sind. Weiterhin haben wir konkrete Anforderungen zu einzelnen Kontrollzielen formuliert. Normalerweise müssen bei einer solchen Verkehrsmessung immer mehrere Telefonanschlüsse zusammen ausgewertet werden, damit keine Rückschlüsse auf einzelne Mitarbeiterinnen oder Mitarbeiter möglich sind. Als Ausnahme von dem Grundsatz sollte für die Telefonzentrale und das Beschwerdetelefon eine separate Messung durchgeführt werden. Wir forderten den Magistrat auf, auf eine Verkehrsmessung in diesen Bereichen zu verzichten beziehungsweise die beiden Organisationseinheiten in jeweils größere Organisationseinheiten zusammenzufassen. Wir werden dass Verfahren weiter begleiten.

### 10.2 Umstellungen von bargeldlosen Zahlungen auf ein einheitliches europäisches Verfahren

SEPA (Single Euro Payments Area) ist die Bezeichnung für einen einheitlichen Euro-Zahlungsverkehrsraum. Das Ziel besteht darin, bargeldlose Zahlungen innerhalb der Teilnehmerländer so zu standardisieren, dass für die Bankkundinnen und Bankkunden keine Unterschiede mehr zwischen nationalen und grenzüberschreitenden Zahlungen bestehen. Im März 2012 trat die Verordnung 260/2012 des europäischen Parlaments und des Rates zur Festlegung der technischen Vorschriften und der Geschäftsanforderungen für Überweisungen und Lastschriften in Euro in Kraft. Die Verordnung legt unter anderem einen Endtermin für die nationalen Überweisungsverfahren und Lastschriftverfahren sowie einen Starttermin für die Internationale Bankkontonummer (IBAN International Bank Account Number) fest. Dem entsprechend müssen die Kernverfahren bei der Senatorin für Finanzen und der Landeshauptkasse sowie die dezentralen Fachverfahren technisch umgestellt werden. Organisatorische Umstellungen sind beispielsweise im Bereich Lastschrift erforderlich. Aufgrund der gesetzlichen Anforderungen müssen die bisherigen Kontonummern und Bankleitzahlen durch IBAN-Nummern und international gültige Bankleitzahlen BIC (Bank Identifier Code) ersetzt werden. In den allermeisten Fällen können die Nummern automatisch durch ein Konvertierungstool umgestellt werden. Wie mit den restlichen Fällen umgegangen wird, ist noch nicht abschließend geklärt. Das herkömmliche Lastschrifteinzugsverfahren wird abgeschafft und durch das SEPA-Lastschrifteinzugsverfahren ersetzt. Die Einzugsermächtigung wird voraussichtlich neu erteilt werden müssen, diese Frage ist aber noch nicht abschließend entschieden. Für das neue Verfahren SEPA erwarten wir eine Verfahrensbeschreibung mit Benennung der technischen und organisatorischen Maßnahmen. Die Datenschutzkonzepte bestehender Verfahren sind anzupassen. Die Mandantsverwaltung wird voraussichtlich zentral erfolgen. Ein Datenschutzkonzept ist auch hier vorzulegen. Wir werden das Projekt weiterhin begleiten.

## 11. Medien/Telemedien

### 11.1 Runder Tisch Digitale Kultur und Schule

Im Berichtsjahr tagte der Runde Tisch „Digitale Kultur und Schule“ mehrfach. In einer der Sitzungen referierten wir über das Thema „Digitale Schule und Datenschutz“. Im Anschluss an diese Sitzung hat sich eine kleine Gruppe gebildet, die nunmehr eine Handlungsorientierung für den Einsatz sozialer Netzwerke durch Lehrkräfte erarbeitet (siehe Ziffer 8.2 dieses Berichts).

Als weiteres datenschutzrechtlich wichtiges Thema wurde vom Zentrum für Medien des Landesinstituts für Schule der Entwurf eines neuen Bildungsplans für die Medienbildung vorgestellt. Dieser basiert auf einem entsprechenden Beschluss der

Kultusministerkonferenz und beinhaltet auch wesentliche Elemente des Datenschutzes. Der Entwurf enthält insbesondere spezifische Anforderungen für die Primarstufe, Sekundarstufe I und Sekundarstufe II.

### 11.2 facebook-Fanseiten

Wir haben bereits im letzten Jahresbericht über die Problematik, die beim Betreiben einer sogenannten Fanseite (siehe 34. Jahresbericht, Ziffer 12.5) bei dem sozialen Netzwerk facebook sowie beim Einsatz des „Gefällt-mir"-Knopfs entsteht, berichtet. Die Betreiber einer solchen Fanseite sind Diensteanbieter nach dem Telemediengesetz und müssen daher bestimmte Pflichten erfüllen. Sie müssen unter anderem Nutzerinnen und Nutzern der Fanseiten (also auch denen, die nicht Mitglied bei facebook sind) ausreichende Informationen über die Datenverarbeitung zur Verfügung stellen und darauf basierend die Einwilligung der Betroffenen zur Datenverarbeitung einholen. Da facebook selber keine ausreichende Information über die Verarbeitung zur Verfügung stellt und den Fanseitenbetreibern keinerlei Verfügungsgewalt über die Daten ihrer „Fans" und die Daten Dritter, die nicht Mitglied im sozialen Netzwerk sind, zugesteht, verstoßen die Fanseitenbetreiber als verantwortliche Stelle gegen die geltenden Datenschutzvorschriften. Mit dem Einrichten einer Fanseite wird automatisch eine regelmäßige Nutzungsanalyse von facebook erstellt (mit Hilfe der Anwendung „facebook insights"), die den Betreibern von Fanseiten in aufbereiteter Form zur Verfügung gestellt wird. Für facebook ist die Analyse für Mitglieder des Netzwerkes personenbezogen und widerspricht damit dem Telemediengesetz, das solche personenbezogenen Nutzungsprofile untersagt. Die Betreiber von Fanseiten haben weder Einfluss auf diese Vorgänge noch Verfügungsgewalt über die Daten, sodass das Betreiben einer Fanseite insoweit rechtswidrig ist. Auch die Integration des „Gefällt-mir"-Knopfs ist aus diesen Gründen nicht datenschutzkonform und fällt in die Verantwortung der jeweiligen Internetseitenbetreiber, die den Knopf integrieren.

Wir haben in diesem Jahr wieder zahlreiche Gespräche mit öffentlichen und nicht öffentlichen Stellen geführt und die bestehende Problematik erläutert und auf die Rechtswidrigkeit hingewiesen.

Im öffentlichen Bereich haben wir unsere Gespräche mit der Senatorin für Finanzen weitergeführt, deren Bemühungen, mit facebook ins Gespräch über die datenschutzkonforme Gestaltung der Fanseiten zu kommen, nicht erfolgreich waren. Die Senatorin für Finanzen hat zugesagt, eine Senatsvorlage vorzubereiten, mit der das Abschalten der Fanseiten bremischer öffentlicher Stellen festgeschrieben wird. Dies begrüßen wir ausdrücklich, erwarten aber auch zügiges Handeln der Beteiligten.

Auch im nicht öffentlichen Bereich haben wir – oft nach Beschwerden von Betroffenen oder Presseberichten – zahlreiche Gespräche geführt und darauf verwiesen, dass es sich bei Betreibern einer Fanseite und bei der Nutzung des „Gefällt-mir"-Knopfs um einen Datenschutzverstoß handelt. Wir planen im kommenden Jahr unsere Aktivitäten im nicht öffentlichen Bereich verstärkt auszubauen.

### 11.3 Veröffentlichungen von Fotos und Namen im Internet

Auch im Berichtsjahr erreichten uns Beschwerden zu Fotos oder persönlichen Informationen im Internet, die ohne Einwilligung oder sogar ohne Kenntnis der Betroffenen veröffentlicht wurden. Unerheblich ist, ob dies aus Unkenntnis oder böser Absicht geschieht. Grundsätzlich gilt: Wer Fotos oder persönliche Informationen von Dritten auf einer Internetseite, in sozialen Netzwerken oder in Foren veröffentlichen möchte, benötigt hierfür die Einwilligung der oder des Betroffenen, solange die Daten nicht allgemein zugänglich sind und das schutzwürdige Interesse der oder des Betroffenen nicht überwiegt. Andernfalls sind die Daten unzulässig gespeichert und daher zu löschen.

In einem Fall wurde eine E-Mail, die persönlich an den Empfänger gerichtet war, auf einer Internetseite veröffentlicht. Hieraus waren nicht nur persönliche Informationen über den Absender erkennbar, sondern es wurden auch falsche Informationen über den Absender ergänzt. In diesem Fall wurden nach unserem Tätigwerden alle Informationen anonymisiert beziehungsweise gelöscht.

Diverse Anfragen und Beschwerden erreichten uns zu Fotos und Informationen, die in sozialen Netzwerken über Dritte veröffentlicht wurden. Auch in dem vermeintlich privaten Bereich eines sozialen Netzwerks ist für die Veröffentlichung von

Fotos die Einwilligung der Betroffenen erforderlich. Denn gerade Fotos werden oft mit anderen Nutzerinnen und Nutzern geteilt oder in öffentlichen oder halb öffentlichen Bereichen zugänglich gemacht und verlassen so den privaten Bereich.

Auch E-Mails, die zwischen zwei Behörden zu einer Bürgeranfrage ausgetauscht wurden und dann ohne Einwilligung der einen Behörde an die betreffenden Bürgerinnen oder Bürger weitergeleitet und von diesen im Internet veröffentlicht wurden, sind – sofern personenbezogene Daten enthalten sind – vor der Veröffentlichung zu anonymisieren.

In einem anderen Fall veröffentlichte eine Behörde Informationen zu einem Verwaltungsverfahren für ein Bauvorhaben im Internet. Die personenbezogenen Informationen wurden in dem entsprechenden Dokument geschwärzt – allerdings so, dass sie für Suchmaschinen sichtbar blieben und somit von Google und anderen Suchmaschinen indexiert (also mit Schlagworten versehen) wurden und in Suchergebnislisten zu den Namen der Betroffenen auftauchten. Diese Panne wurde nach Kenntnisnahme sofort behoben.

Schwierig wird es für die datenschutzrechtlichen Aufsichtsbehörden, wenn personenbezogene Informationen auf Internetseiten veröffentlicht werden, die keine oder keine vollständigen Betreiberinformationen vorhalten. Oft handelt es sich auch um Dienste, die außerhalb der Europäischen Union betrieben werden und somit für deutsche Aufsichtsbehörden schwer greifbar sind.

### 11.4 Überprüfung von Apps

Applikationen (Anwendungsprogramme für Smartphones und Tablet-Computer), kurz Apps, für mobile Endgeräte spielen eine immer größer werdende Rolle für Nutzerinnen und Nutzer. Die kleinen Anwendungen erleichtern in der Regel den Zugang auf bestimmte Internetangebote, aber ermöglichen oft einen weitreichenden Zugriff auf Daten der Nutzerinnen und Nutzer, die auf den Smartphones (Mobiltelefonen, die über eine große Menge Computerfunktionalität verfügen), Tablet-Computern (tragbaren, flachen Computer, die in der Regel durch Gesten der Benutzerinnen und Benutzer gesteuert werden) und anderen mobilen Endgeräten gespeichert sind. Mangelnde Transparenz und pauschale Freigaben durch ahnungslose Nutzerinnen und Nutzer „ermöglichen“ den Apps einen weitreichenden Zugriff auf die auf dem Endgerät gespeicherten Kontaktdaten, Kalenderfunktionen oder Standortdaten und spähen somit die Daten der Betroffenen sowie deren Kontakte aus.

Uns erreichte eine Anfrage zu einer von einem bremischen Unternehmen angebotenen App zur Verkehrsverbindungsauskunft mit der Bitte zur datenschutzrechtlichen Überprüfung. Die Applikation umfasst neben der Auskunft von Fahrplandaten auch eine sogenannte Echtzeitinformation zu Verspätungen oder Ausfällen von Verbindungen. Die Verbindungsauskunft kann mit Hilfe der aktuellen Position (Global Positioning System, kurz GPS) oder durch Übernahme einer Adresse aus dem lokalen Adressbuch erfolgen, sodass hier auch Standortdaten und Kontaktdaten genutzt werden. Während der Überprüfung ergab sich, dass diese Daten aber vor der Verarbeitung durch die Betreiber anonymisiert wurden. Die datenschutzrechtlichen Mängel, die bei der Überprüfung deutlich wurden, konnten im Verfahren behoben werden.

Grundsätzlich ist bei der Auswahl von Apps davon abzuraten, ungeprüfte Applikationen auf einem Endgerät zu installieren und den Anwendungen weitreichende Zugriffe auf personenbezogene Daten wie Kontakte oder Kalendereinträge zu erlauben, denn viele Apps verschaffen sich – oft ohne Wissen der Nutzerinnen und Nutzer – Zugriff auf Daten, die zur eigentlichen Anwendung nicht erforderlich sind und speichern diese Daten unberechtigterweise auf den Servern der Betreiber.

### 11.5 Projektarbeiten in Schulen zum Thema „Soziale Netzwerke“

Soziale Netzwerke spielen in unserer Gesellschaft eine große Rolle und werden zunehmend kritisch diskutiert. Insbesondere der Umgang mit personenbezogenen Daten, die oft mangelhaften Schutzmöglichkeiten der Privatsphäre und die fehlende Transparenz stehen im Fokus der Debatte. Wir haben uns daher besonders über verschiedene Anfragen von Schülerinnen und Schülern gefreut, die sich im Rahmen von Projektwochen oder Halbjahresarbeiten mit sozialen Netzwerken und deren Risiken auseinandergesetzt haben. Wir haben spannende und informative Diskus-

sionen mit den Schülerinnen und Schülern erlebt, in denen deutlich wurde, dass auch die „digital natives“ („digitale Eingeborene“ sind Personen, die mit digitalen Technologien aufgewachsen sind) durchaus kritisch im Umgang mit ihren Daten sind.

### 11.6 Erstellung von Verfahrensbeschreibungen und eines Rahmendatenschutzkonzeptes für bremen.de

Das offizielle Stadtportal der Freien Hansestadt Bremen www.bremen.de stellt nicht nur Informationen für Nutzerinnen und Nutzer auf der Webseite bereit, sondern verarbeitet auch ihre personenbezogenen Daten in zahlreichen Verfahren. So werden in Angeboten wie Bremen-Mail (ein Webmail-Angebot), dem Kleinanzeigenmarkt auf dem sogenannten Schwarzen Brett oder den Visitenkarten personenbezogene Daten erhoben, verarbeitet und gespeichert. In diesem Jahr haben wir die bremen.online GmbH bei der Erstellung der Verfahrensbeschreibungen und dem Rahmendatenschutzkonzept beraten und den Prozess aktiv begleitet. Dabei ist deutlich geworden, dass zusätzliche technische und organisatorische Maßnahmen erforderlich sind (zum Beispiel das Erstellen von Löschkonzepten zum regelmäßigen Löschen der nicht mehr erforderlichen Daten), um den Schutz der auf www.bremen.de erhobenen personenbezogenen Daten gewährleisten zu können. Leider konnte der Prozess bisher nicht abgeschlossen werden und wurde immer wieder zeitlich verzögert. Wir erwarten nun, dass die Verfahrensbeschreibungen und insbesondere das Rahmendatenschutzkonzept zeitnah fertiggestellt werden und auch bei Neueinführungen und Änderungen von Verfahren die Vorgaben erfüllt werden, um so den datenschutzgerechten Betrieb des Stadtportals sicherzustellen.

### 11.7 Orientierungshilfe „Soziale Netzwerke“

Die Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich der Länder Hamburg, Bayern, Bremen, Mecklenburg-Vorpommern, Sachsen und Schleswig-Holstein haben im Berichtsjahr eine Orientierungshilfe zum Thema „Soziale Netzwerke“ erarbeitet. Die Orientierungshilfe soll den datenschutzgerechten Einsatz von sozialen Medien, insbesondere sozialen Netzwerken, ermöglichen. Der Bedarf für eine Orientierungshilfe zur Verwendung sozialer Netzwerke im professionellen Rahmen ist in der Vergangenheit immer deutlicher geworden; daher richtet sich die Orientierungshilfe hauptsächlich an Betreiber sozialer Netzwerke, Behörden und Unternehmen, die mit sozialen Netzwerken ihre Aufgaben erfüllen oder ihre Geschäftszwecke verfolgen. Für private Nutzerinnen und Nutzer sind zwar bereits einige Leitfäden oder Checklisten erarbeitet worden (siehe zum Beispiel unter http://www.datenschutz.de), jedoch erfordert die oft vorhandene Unwissenheit und Unsicherheit bei der professionellen Nutzung aus Sicht der Aufsichtsbehörden diese Orientierungshilfe. Unter den Begriff des professionellen Nutzers fallen zum Beispiel öffentliche Stellen, die mithilfe von sozialen Medien den Bürgerkontakt verbessern, themenbezogene Umfragen im Internet umsetzen oder in bestehenden sozialen Netzwerken aktiv im Rahmen ihrer Nachwuchsgewinnung nutzen möchten, aber auch Unternehmen, die sich im Web 2.0 präsentieren.

In der Orientierungshilfe wird bewusst auf eine getrennte Darstellung von rechtlichen und technischen Anforderungen verzichtet, um eine praxisnahe Orientierung geben zu können. Daher werden anhand der Schutzziele der Datensicherheit und des Datenschutzes – Vertraulichkeit, Integrität, Verfügbarkeit, Intervenierbarkeit, Transparenz und Nichtverkettbarkeit – die Mindeststandards konkretisiert und bestehende datenschutzkonforme Ansätze aufgezeigt. Als Grundlage dienen die bestehenden gesetzlichen Vorgaben und die Beschlüsse und Entschließungen der nationalen und internationalen datenschutzrechtlichen Gremien. Die Orientierungshilfe ist aktuell in der Abstimmung und wird voraussichtlich Anfang 2013 veröffentlicht.

### 11.8 Bericht aus dem Arbeitskreis Medien

Der Arbeitskreis Medien tagte in diesem Jahr zweimal und beschäftigte sich sowohl mit Themen des öffentlichen wie auch des nicht öffentlichen Bereiches.

Übergreifend für beide Bereiche wurden die Datenschutzmängel bei Web 2.0-Angeboten diskutiert. Diese Angebote werden oft sowohl von öffentlichen als auch von nicht öffentlichen Stellen bedenkenlos eingesetzt, obwohl viele personen-

bezogene Daten der Nutzerinnen und Nutzer unzulässigerweise verarbeiten. Schwerpunktmäßig wurden im Arbeitskreis die unterschiedlichen Aktivitäten der Aufsichtsbehörden gegenüber facebook abgestimmt und begleitet.

Im nicht öffentlichen Bereich ist die Ausgestaltung der Verarbeitung personenbezogener Daten bei IPTV (Internet Protocol Television, allgemeine Bezeichnung für Fernsehprogramme und Filme, die über das Internet übertragen werden) diskutiert worden. Auch die Verarbeitung personenbezogener Daten durch Anbieter von Telemedien zu Werbezwecken war Thema im Arbeitskreis, insbesondere hinsichtlich der Anwendung der sogenannten Cookie-Richtlinie der Europäischen Union (Richtlinie 2002/58), die die aktive Einwilligung der Nutzerinnen und Nutzer erfordert, bevor ein Cookie auf dem eigenen Computer abgelegt wird. Die Artikel-29-Gruppe hat zu dieser Fragestellung ein Arbeitspapier veröffentlicht, dem sich die Aufsichtsbehörden grundsätzlich anschließen.

Weitere Themen waren neben datenschutzrechtlichen Bewertungen von Smartphones und Apps auch die neue, im Umgang mit personenbezogenen Daten mangelhafte Datenschutzerklärung des Anbieters Google.

### 11.9 Bericht aus dem Arbeitskreis Schule und Bildung

Anlässlich der Sitzungen des Arbeitskreises Schule und Bildung wurde der Entwurf der Datenschutz-Grundverordnung der Europäischen Union erörtert. Danach sollen sowohl die Mitgliedsstaaten als auch die Aufsichtsbehörden Medienkompetenzen vermitteln und dabei auch den Minderjährigenschutz im Internet thematisieren. Der Arbeitskreis hält es für notwendig, den Datenschutz als Bildungsaufgabe deutlicher in den Verordnungsentwurf aufzunehmen.

Weitere Themen waren:

— Datenschutz in Lehrplänen,

— Einsatz sozialer Netzwerke im Unterricht,

— Sachstand über die Beratungen der Enquete-Kommission des Deutschen Bundestages zum Internet in der digitalen Gesellschaft,

— Bericht über einen wissenschaftlichen Workshop an der Universität Koblenz zur Medienkompetenz von Schülerinnen und Schülern sowie Studierenden,

— aktuelle Studien des Medienpädagogischen Forschungsverbundes Südwest.

## 12. Beschäftigtendatenschutz

### 12.1 Öffentlicher Bereich

#### 12.1.1 Umstellung der Personalakten auf elektronische Akten

Nach unseren Informationen plant insbesondere die Universität Bremen, die Personalgrundakten entsprechend umzustellen. Wir haben daher die Senatorin für Finanzen als oberste Dienststelle für Personal darauf hingewiesen, dass das Bremische Beamtengesetz die Umstellung von Personalakten auf elektronische Akten nur zur Personalverwaltung oder Personalwirtschaft erlaubt. Eine weitere Einschränkung gibt es bei den Unterlagen über medizinische oder psychologische Untersuchungen und Tests. Hier dürfen im Rahmen der Personalverwaltung die Ergebnisse nur automatisiert verarbeitet und genutzt werden, soweit sie die Eignung betreffen und ihre Verarbeitung oder Nutzung dem Schutz der Betroffenen dient.

Unter Hinweis auf die amtliche Begründung zur insoweit identischen Regelung im Bundesbeamtengesetz halten wir vor einer derartigen Umstellung die Aufnahme besonderer Regelungen in die Verwaltungsvorschrift über die Erhebung von Personalaktendaten und die Führung von Personaldateien für erforderlich. Die wesentlichen Punkte für eine solche Verwaltungsvorschrift sind aus datenschutzrechtlicher Sicht:

— Einhaltung des Grundsatzes der Eindeutigkeit der Personalakte durch entsprechende Aktenführung,

— keine Einschränkung der Einsichtsrechte der Beschäftigten,

— Vermeidung paralleler Aktenführung in Papierform und elektronischer Form,

— Einsatz ausschließlich elektronisch geführter Personalgrundakten nur bei Vorliegen einer qualifizierten Signatur nach dem Bremischen Verwaltungsverfahrensgesetz und dem Signaturgesetz zur Gewährleistung der Beweiskraft elektronisch gespeicherter Urkunden,

— manipulationssicheres Einscannen von Personalaktendaten,

— Scannen und Signieren der Personalakten sowie Digitalisierung neuer Vorgänge ausschließlich durch Beschäftigte der Personalstelle,

— Maßnahmen und Entscheidungen, wenn beim Einscannen Originale der Personalaktendaten während des Scanprozesses beschädigt oder zerstört werden oder ein Originaldokument verloren geht,

— Dokumentation zur Nachvollziehbarkeit von Fehlerfällen beim Einscannen,

— vollständige Sichtprüfung mit qualifizierter Signatur der eingescannten Originaldokumente und anschließende Vernichtung der Papierakten,

— schriftliche Festlegung, welche Teile der Personalakte in welcher Form nicht vollständig in Schriftform oder vollständig elektronisch geführt werden,

— Dokumentation im vollständigen Verzeichnis aller Teilakten und Nebenakten, welche Teile der Personalakte in welcher Form geführt werden,

— allgemeine Bekanntgabe über die Verarbeitungsformen der Personalakten.

Wir haben die Senatorin für Finanzen gebeten, die Verwaltungsvorschrift vorher entsprechend zu ergänzen. Durch die Umsetzung unserer Vorgaben werden die Gefahren für die Rechte der Beschäftigten bei dieser Umstellung reduziert. Gleichwohl bedarf es bei der Umstellung einer Vorabkontrolle, die auch die Gestaltung und Auswahl von Datenverarbeitungssystemen für elektronische Personalakten beinhaltet (Datensparsamkeit und Datenvermeidung sowie Aufbewahrungsfristen und Löschungsfristen). Eine Antwort, ob unsere Vorgaben umgesetzt werden, steht noch aus.

### 12.1.2 Offenbarung von Beschäftigtendaten in einer Personalversammlung durch die Pflegedienstleitung

Die Leitung eines Pflegedienstes im Klinikum Bremen-Mitte hatte auf einer Personalversammlung den Anwesenden offenbart, in welcher Reihenfolge welche Beschäftigten von einer Personaleinsparung betroffen sind. Wir wiesen darauf hin, dass es sich hierbei um eine unzulässige Offenbarung von Beschäftigtendaten handelte. Es hätte in diesem Fall gereicht, wenn nur die oder der jeweils Betroffene über ihre oder seine eigenen Daten im Ranking zur Personalreduktion informiert worden wäre.

Wir haben das Klinikum Bremen-Mitte gebeten, sicherzustellen, dass eine derartige Offenbarung von Personaldaten zukünftig unterbleibt, indem die Pflegedienstleitungen des Klinikums darüber unterrichtet und entsprechend angewiesen werden. Dies hat uns die pflegerische Geschäftsführung inzwischen bestätigt.

### 12.1.3 Übersendung der Personalakten einschließlich der Krankenakten bei Bewerbungen innerhalb der bremischen Verwaltung

Beschäftigte der Freien Hansestadt Bremen werden bei internen Bewerbungen bereits durch den Ausschreibungstext und vor Beginn des Personalauswahlverfahrens aufgefordert, in die Vorlage ihrer Personalakte gegenüber der ausschreibenden Stelle einzuwilligen. Hierzu wird regelmäßig auch die Krankenakte als Teilakte der Personalakte einbezogen. Die Übersendung der Personalgrundakte, der Teilakten und der Nebenakten bei einer Bewerbung innerhalb der bremischen Verwaltung halten wir aus folgenden Gründen nicht für zulässig:

Das Bremische Beamtengesetz enthält Regelungen zur Vorlage von Personalakten durch die Personalakten führende Stelle an andere Behörden. Danach darf die Personalakte für Zwecke der Personalverwaltung einer anderen Behörde vorgelegt werden, soweit diese an einer Personalentscheidung, in diesem Fall der Entscheidung über die Personalauswahl, beteiligt ist. Hier gilt wie überall das Verhältnismäßigkeitsprinzip, das heißt die Datenübermittlung muss geeignet, erforderlich

und angemessen sein. Wir halten im Bewerbungsverfahren ausschließlich die Übermittlung der Inhalte der Grundakte für verhältnismäßig. Soweit eine Auskunft ausreicht, ist von einer Vorlage abzusehen.

Mangels rechtlicher Grundlage für eine Personalakteneinsicht, auch in Teilakten und Nebenakten, müsste eine wirksame Einwilligung vorliegen. Eine Einwilligung ist nach dem Bremischen Datenschutzgesetz nur wirksam, wenn sie auf der freien Entscheidung der oder des Betroffenen beruht. Freiwilligkeit ist nur zu bejahen, wenn die Einwilligung nicht in einer Zwangslage oder unter Druck getroffen wurde.

Einerseits hat sich die oder der Betroffene freiwillig um die Stelle beworben, ist nicht dazu verpflichtet gewesen, den Arbeitsplatz zu wechseln, hat sich bewusst dem Bewerbungsverfahren gestellt und in die Weitergabe der Personalakte eingewilligt. Andererseits ist es für die Freiwilligkeit der Einwilligung erforderlich, dass die oder der Betroffene die Datenübermittlung verweigern oder eine zuvor erteilte Einwilligung widerrufen kann, ohne erhebliche Nachteile befürchten zu müssen. Uns sind Fälle bekannt, in denen Betroffene, die ihre Einwilligung nur auf Grundakten erstrecken wollten, den Hinweis von Behörden erhielten, in diesem Fall könne ihre Bewerbung nicht berücksichtigt werden.

Für Bewerberinnen und Bewerber um eine andere Stelle besteht daher keine andere Möglichkeit, als der Weitergabe dieser Teile der Personalakte zuzustimmen. Es handelt sich hier also um einen faktischen Zwang. Daher erfolgt die Einwilligung in die Weitergabe der Krankenakte und der übrigen Teil- und Nebenakten nicht freiwillig und ist demzufolge nicht wirksam.

Darüber hinaus halten wir die Vorlage von Teil- und Nebenakten oder Auskünfte hieraus regelmäßig nicht für erforderlich. Insbesondere hinsichtlich der Krankenakte können schutzwürdige Belange der oder des Betroffenen erheblich beeinträchtigt werden. Dies ist besonders der Fall, soweit die Krankenakte außergewöhnliche beziehungsweise überdurchschnittlich viele Krankentage der letzten drei Jahre dokumentiert. Nach einschlägigen Untersuchungen zur Gesundheitsförderung am Arbeitsplatz sind etwa 40 Prozent aller Erkrankungen arbeitsbedingt. Daraus ist zu schließen, dass derartige Erkrankungen durch einen Arbeitsplatzwechsel beseitigt oder erheblich vermindert werden können. Insoweit sind Informationen über die Anzahl der Krankentage der letzten drei Jahre auf einem bestimmten Dienstposten zur Prüfung der gesundheitlichen Eignung für den zu besetzenden Dienstposten nicht geeignet.

Wir haben der Senatorin für Finanzen in ihrer Funktion als oberste Dienstbehörde für Personal unsere Auffassung dargelegt und sie gebeten mitzuteilen, ob sie unsere Auffassung teilt. Für diesen Fall haben wir sie gebeten, die Behörden und sonstigen ihrer Aufsicht unterliegenden öffentlichen Stellen auf die Rechtslage hinzuweisen und zu bitten, auf die Einholung einer derartigen Einwilligung und den Hinweis zur Einwilligungserklärung in den Stellenausschreibungen zu verzichten.

Die senatorische Behörde hat erklärt, ein Verstoß gegen den Grundsatz der Erforderlichkeit wegen der Besonderheit des Beamtenverhältnisses oder Arbeitsverhältnisses zu einem öffentlichen Arbeitgeber erkenne sie nicht. Der neue Dienstherr oder Arbeitgeber müsse sich vor der Auswahlentscheidung ein umfassendes Bild über die Bewerberin oder den Bewerber verschaffen. Dies gelte auch für interne Bewerbungen und geschehe regelmäßig anhand der Bewerbungsunterlagen, aktueller Beurteilungen und durch Einsicht in die Personalakte. Die Personalakte umfasse neben der Grundakte auch alle Teilakten wie beispielsweise die Krankenakte und bilde den bisherigen beruflichen Werdegang ab. Auch wenn Bewerberinnen und Bewerber bereits im bremischen öffentlichen Dienst beschäftigt seien, obliege dem Dienstherrn beziehungsweise Arbeitgeber die Verpflichtung der Bestenauslese aufgrund des Anforderungsprofils der ausgeschriebenen Stelle. Dabei sei die Einsichtnahme in die gesamte Personalakte ein wesentlicher Bestandteil des Auswahlverfahrens. Die in der Akte dokumentierte bisherige berufliche Entwicklung und der Eindruck über die Persönlichkeit ermöglichten eine fundierte Eignungsprognose für die Ausübung des angestrebten neuen Dienstpostens.

Die Bewerbung erfolge freiwillig, und die Abgabe der Einverständniserklärung werde nach wie vor nicht von allen Dienststellen gefordert. Nach Informationen der Senatorin für Finanzen würde die Personalakte erst dann zur Einsichtnahme von den Beschäftigungsdienststellen angefordert, wenn die Bewerberin oder der Bewerber in die engere Wahl gelangt sei. Spätestens zu diesem Zeitpunkt müsse

es der oder dem zuständigen Dienstvorgesetzten möglich sein, umfassende Kenntnisse über die jeweiligen Bewerberinnen und Bewerber zu erlangen, um eine sachgerechte Auswahlentscheidung treffen zu können. Das Vorliegen der Einverständniserklärung zur Einsichtnahme in die Personalakte beschleunige daher den Verfahrensablauf.

Wir haben der senatorischen Behörde entgegnet, sie habe zur Besonderheit des Beamtenverhältnisses oder Arbeitsverhältnisses nichts ausgeführt. Dagegen haben wir auf die materiell rechtlich identische Regelung im Bundesdatenschutzgesetz zur Verarbeitung von Beschäftigtendaten sowohl für die Beschäftigten der Privatwirtschaft als auch der Bundesverwaltung und auf das von der Rechtsprechung des Bundesarbeitsgerichts entwickelte Fragerecht des Arbeitgebers hingewiesen, die für beide Bereiche beachtlich sei. Außerdem haben wir erhebliche Zweifel, dass durch die Inhalte der Urlaubs- und Krankenakte geeignete Erkenntnisse über den beruflichen Werdegang über Bewerberinnen und Bewerber erlangt werden können. Besonders bedauerlich ist, dass das Ressort nicht auf unsere vorgenannten Argumente zu der Beeinträchtigung schützwürdiger Belange der Betroffenen eingegangen ist. Aus diesen Gründen haben wir die Senatorin für Finanzen gebeten, unsere Gesichtspunkte einer erneuten Prüfung zuzuführen.

### 12.1.4 Bericht aus dem Arbeitskreis Personalwesen

Der Arbeitskreis Personalwesen beriet über den seinerzeitigen Stand zum Gesetzentwurf über den Beschäftigtendatenschutz. Darüber hinaus wurden Anforderungen zur elektronischen Personalakte (siehe Ziffer 12.1.1 dieses Berichts) erörtert. Weitere Themen waren insbesondere

— Nutzung sozialer Netzwerke durch Personalstellen,

— Beendigung des Projekts ELENA (Elektronisches Entgeltnachweisverfahren),

— BEM (Betriebliches Eingliederungsmanagement),

— Polizeiliches Bewerberauswahlverfahren,

— Datenaustausch zwischen Beihilfestellen und Krankenkassen,

— Bestellung oder Beauftragung externer Betriebsärztinnen und Betriebsärzte.

Die Aufgaben der Aufsichtbehörden für den nicht öffentlichen Bereich sind inzwischen auf die Landesbeauftragen für den Datenschutz in den jeweiligen Bundesländern übertragen worden. Daher war es zweckmäßig, die für den Datenschutz in der Privatwirtschaft zuständige Arbeitsgruppe Beschäftigtendatenschutz mit dem Arbeitskreis Personalwesen zusammenzulegen. Aus diesem Grund wird jetzt der Arbeitskreis Beschäftigtendatenschutz alle mit diesem Thema zusammenhängenden Fragen beraten, unabhängig davon, ob es sich um Probleme aus der Privatwirtschaft oder dem öffentlichen Dienst handelt.

## 12.2 Nicht öffentlicher Bereich

### 12.2.1 Übermittlung der Rentenversicherungsnummern von Beschäftigten an eine Krankenkasse für einen Gesundheitsbericht

Ein Unternehmen übermittelte die Rentenversicherungsnummern von fast 3.000 Beschäftigten an eine Betriebskrankenkasse. Diese Angaben wurden mit der Information über die Arbeitsbereiche, in denen die Betroffenen eingesetzt sind, verbunden. Die Krankenkasse erstellte auf der Basis dieser Daten einen Gesundheitsbericht. Dieser Bericht wurde im unternehmenseigenen Intranet veröffentlicht. Durch die Aufteilung in einzelne Unternehmensbereiche konnte beispielsweise ersehen werden, in welchen Bereichen welche (auch psychische) Erkrankungen besonders häufig auftreten. Der kleinste Bereich umfasste eine Personenzahl von 34 Beschäftigten.

Auf unsere Anfrage erklärte das Unternehmen, die vorgenannte Datenübermittlung würde jährlich für die Erstellung des Gesundheitsberichts erfolgen. Es seien keine Namen, sondern lediglich die Rentenversicherungsnummern an die Krankenkasse übermittelt worden. Dies seien anonymisierte Daten. Die Gesundheitsberichte würden einen Aufschluss darüber geben, ob bestimmte Erkrankungen aufgrund von Maßnahmen zur Gesundheitsförderung im Unternehmen zurückgegangen seien.

Die Rentenversicherungsnummer setzt sich nach dem Fünften Sozialgesetzbuch im Wesentlichen aus dem Geburtsdatum, den Anfangsbuchstaben des Geburtsnamens und Aussagen über das Geschlecht zusammen. Demzufolge ist die Rentenversicherungsnummer ein personenbezogenes Datum. Arbeitgeber dürfen nach diesem Gesetz die Rentenversicherungsnummer nur für die dort abschließend aufgeführten Zwecke verwenden. Die Nutzung für die Erstellung von Gesundheitsberichten gehört nicht dazu. Die Datenübermittlung war daher unzulässig.

Wir forderten das Unternehmen auf, diese Datenübermittlung zukünftig zu unterlassen. Außerdem drangen wir darauf, die Betriebskrankenkasse darüber zu unterrichten, dass unzulässig übermittelte personenbezogene Daten beim Empfänger zu löschen sind. Daher musste das Unternehmen die Krankenkasse veranlassen, diese Daten zu löschen. Des Weiteren mussten im Intranet des Unternehmens die Teile des aktuellen Gesundheitsberichts und der bisherigen Gesundheitsberichte, die einen Personenbezug aufweisen können, gelöscht werden.

Das Unternehmen hat inzwischen erklärt, die Anforderungen umgesetzt zu haben. Wir haben ein Ordnungswidrigkeitenverfahren gegen das Unternehmen wegen der unzulässigen Datenübermittlung an die Krankenkasse eingeleitet.

### 12.2.2 Videoüberwachung der Beschäftigten beim Beladen und Entladen von Waren

Im Lagerraum einer Firma war eine Videokamera auf ein Rolltor gerichtet, an dem die Lieferfahrzeuge beladen und entladen werden. Dadurch waren die Beschäftigten bei diesen Tätigkeiten einer Videoüberwachung ausgesetzt. Zugriff auf die Videoaufzeichnungen hatte der Geschäftsführer. Er begründete die Überwachung damit, dass dadurch schnelle medizinische Hilfe bei Unfällen während dieser Tätigkeiten geleistet werden könne. Außerdem sei die Überwachung zum Schutz der Betroffenen vor Übergriffen von außen erforderlich. Anlässlich einer Überprüfung vor Ort ließ der Geschäftsführer diese beiden Gründe fallen und gab stattdessen als einzigen neuen Zweck die Vorbeugung vor Diebstahl an.

Wir wiesen den Geschäftsführer darauf hin, dass die Videoüberwachung nicht erforderlich war und damit gegen die einschlägige Vorschrift des Bundesdatenschutzgesetzes verstieß. Beim Beladen und Entladen der Lieferfahrzeuge sind regelmäßig ein Lieferant und eine Beschäftigte oder ein Beschäftigter der Firma anwesend. Regelmäßig dürften dabei nach kaufmännischen Grundsätzen die Warenausgabe und der Warenempfang protokolliert und unterschrieben werden. Zudem sind in dem Raum mit dem Rolltor mindestens eine Beschäftigte oder ein Beschäftigter an den insgesamt drei Büroarbeitsplätzen anwesend. Dies stellt eine angemessene Vorbeugung gegen Diebstahl dar. Außerdem sind die Betroffenen einem Generalverdacht ausgesetzt, sodass ihre schutzwürdigen Interessen gegen die Videoüberwachung überwiegen. Allein dies führt bereits zur Unzulässigkeit der Videoüberwachung. Nach dem Vorortttermin forderten wir den Geschäftsführer auf, die Kamera zu entfernen. Er hat uns dies mittlerweile bestätigt.

### 12.2.3 Veröffentlichung von Beschäftigtendaten und Bildern auf der Homepage der Arbeitgeberin oder des Arbeitgebers

Generell ist es nicht erforderlich, für Zwecke eines Beschäftigungsverhältnisses Daten über Beschäftigte im Internet auf der Homepage der Arbeitgeberin oder des Arbeitgebers zu veröffentlichen. Die Daten sind damit weltweit und jederzeit für alle Nutzerinnen und Nutzer des Internets zugänglich. Soweit Beschäftigtendaten außerhalb des Beschäftigungsverhältnisses veröffentlicht werden sollen, ist dies nach dem Bundesdatenschutzgesetz nur unter engen Voraussetzungen zulässig. Arbeitgeberinnen und Arbeitgeber haben vor der Veröffentlichung der Daten den Zweck konkret festzulegen und dabei zu klären, weshalb für diesen Zweck eine weltweite Veröffentlichung im Internet erforderlich ist.

Des Weiteren haben Arbeitgeberinnen und Arbeitgeber zu prüfen, ob schutzwürdige Interessen der Beschäftigten überwiegen. Hierbei ist zu beachten, dass ins Internet eingestellte Daten regelmäßig von Internetsuchmaschinen sowie Nutzerinnen und Nutzern abgerufen, weltweit und vielfältig verknüpft und verändert werden können. Außerdem können Arbeitgeberinnen und Arbeitgeber nach Wegfall des Zwecks der Veröffentlichung diese Daten nur auf der eigenen Homepage löschen. Sie haben keinen Einfluss mehr auf die Verwendung der Daten durch Dritte. Aus diesen Gründen überwiegen grundsätzlich die schutzwürdigen Inter-

essen der betreffenden Beschäftigten an dem Ausschluss der Veröffentlichung ihrer Daten auf der Homepage von Arbeitgeberinnen und Arbeitgebern.

Eine Veröffentlichung von personenbezogenen Beschäftigtendaten könnte zulässig sein zur Erfüllung eines konkreten Zweckes, soweit sie sich auf Mitglieder der Geschäftsführung beschränken. Diese sind für das Unternehmen verantwortlich und vertreten es auch rechtlich nach außen. Die Veröffentlichung von Fotos oder Bilddaten über Beschäftigte ist regelmäßig nicht erforderlich.

Soweit eine Veröffentlichung von Beschäftigtendaten über deren Einwilligung gerechtfertigt werden soll, ist zu beachten, dass eine Einwilligung nur wirksam ist, wenn sie auf der freien Entscheidung der oder des Betroffenen beruht. Dies ist aber im Beschäftigungsverhältnis regelmäßig nicht der Fall. Beschäftigte sind insoweit abhängig von ihren Arbeitgeberinnen und Arbeitgebern und können erhebliche Nachteile bis hin zur Entlassung befürchten, wenn sie ihre Einwilligung verweigern oder später mit Wirkung für die Zukunft widerrufen. Sollten diese Nachteile aufgrund einer für die Beschäftigten günstigen Situation im Arbeitsleben tatsächlich im konkreten Fall nicht zu befürchten sein, könnte eine Einwilligung wirksam sein, wenn sie tatsächlich auf der freien Entscheidung der oder des Betroffenen beruht. Dies müsste im Einzelfall geklärt werden. Gleichwohl bleibt das Erfordernis, auf das Ausmaß der schriftlich zu erteilenden Einwilligung und insbesondere auf die Risiken hinzuweisen, die eingangs beschrieben werden.

Eine Veröffentlichung von Beschäftigtendaten auf der Homepage der Arbeitgeberin oder des Arbeitgebers ist demnach grundsätzlich nicht zulässig. Allenfalls könnte die Veröffentlichung von Telefondurchwahlnummern für bestimmte Bereiche sowie die räumliche Erreichbarkeit von Beschäftigten ohne Angabe ihrer Namen zulässig sein, soweit dies für einen konkreten Zweck erforderlich ist. E-Mail-Adressen dürfen nur im Internet veröffentlicht werden, soweit sie keine Namensbestandteile der Beschäftigten enthalten.

### 12.2.4 Übermittlung von Daten über Gewerkschaftsmitglieder an den Betriebsrat zur Anpassung des Gewerkschaftsbeitrags

Ein Mitglied einer Gewerkschaft informierte uns darüber, dass seine Mitgliedsdaten ohne seine Einwilligung an den Betriebsrat seiner Firma übermittelt worden seien. Begründet worden sei die Übermittlung mit der Anpassung der Beiträge. Wir legten dem Unternehmen dar, dass Angaben über die Gewerkschaftszugehörigkeit besondere Arten von Daten sind. Sie dürfen nach dem Bundesdatenschutzgesetz nur unter ganz engen Voraussetzungen verarbeitet werden. Danach dürfen Organisationen, die gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, diese Daten nur erheben, verarbeiten und nutzen, soweit sie für die Tätigkeit der Organisation erforderlich sind. Dies gilt auch für personenbezogene Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten. Dazu gehört nicht die Datenübermittlung an einen Betriebsrat zur Anpassung des Gewerkschaftsbeitrags.

Wir haben dem Petenten dargelegt, dass wir seine Eingabe ohne Preisgabe seiner Identität bei seiner Gewerkschaft überprüfen möchten und gebeten, uns den Namen der Organisation zu nennen. Leider ist dies nicht erfolgt.

### 12.2.5 Überprüfung der Richtigkeit von Bewerberdaten

Wir sind gefragt worden, ob und auf welche Art und Weise potentielle Arbeitgeberinnen und Arbeitgeber Bewerberdaten auf ihre Richtigkeit überprüfen dürfen. Nach dem Bundesdatenschutzgesetz dürfen für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses nur die dafür erforderlichen Daten erhoben, verarbeitet und genutzt werden. Grundsätzlich sind die Daten bei der oder dem Betroffenen zu erheben. Dazu gehören Dokumente zum Nachweis der für den zu besetzenden Arbeitsplatz dargelegten Qualifikationsanforderungen, beispielsweise Schulabschluss, Abschluss einer Berufsausbildung oder eines Studiums sowie Beurteilungen durch frühere Arbeitgeber. Eine Datenerhebung ohne Mitwirkung der oder des Betroffenen ist nur zulässig, wenn eine Erhebung bei anderen Stellen oder Personen oder die Erhebung bei der oder dem Betroffenen einen unverhältnismäßigen Aufwand erfordert. Außerdem dürfen hierbei schutzwürdige Interessen der Betroffenen nicht überwiegen.

Nach unseren Erfahrungen in der Beratung und Prüfpraxis bedarf es regelmäßig keiner Erhebung von Bewerberdaten bei Dritten ohne Mitwirkung der oder des

Betroffenen. Dies resultiert aus der Verpflichtung der Bewerberinnen und Bewerber, im Bewerbungsverfahren gegenüber einem potentiellen Arbeitgeber richtigen Angaben auf Fragen zu machen, deren Beantwortung für die Entscheidung über die Besetzung der Stelle erforderlich sind. Auch die Überprüfung der Richtigkeit der Bewerberdaten bei Dritten ist regelmäßig nicht erforderlich. Wenn Zweifel an der Richtigkeit dieser Daten bestehen, ist es für den Arbeitgeber zumutbar, bei der Bewerberin oder dem Bewerber nachzufragen, um Aufklärung zu bitten und sich weitere Belege vorlegen zu lassen.

Dieser Rechtslage stehen die realen Möglichkeiten von Arbeitgeberinnen und Arbeitgebern gegenüber, unter Verstoß gegen das Bundesdatenschutzgesetz Bewerberdaten hinter dem Rücken der Betroffenen zu überprüfen und weitere Daten zu erheben. Hierbei handelt es sich beispielsweise um Datenerhebungen bei früheren Arbeitgebern oder in sozialen Netzwerken. Gerade bei der Recherche über Bewerberinnen und Bewerber im Internet können potentielle Arbeitgeberinnen und Arbeitgeber Angaben erheben, die nicht für die Entscheidung über die Stellenbesetzung erforderlich sind. Dies können häufig auch Angaben sein, die ein Einfallstor für unzulässige Benachteiligungen nach dem Allgemeinen Gleichbehandlungsgesetz sind, beispielsweise ethnische Herkunft, Religion, Weltanschauung, Behinderung oder sexuelle Identität. Daher überwiegen bei Recherchen im Internet ohne Mitwirkung der oder des Betroffenen regelmäßig deren schutzwürdige Interessen, sodass diese Art der Datenerhebung unzulässig ist.

### 12.2.6 Zugriff mehrerer Beschäftigter auf einen PC zur Erfassung der Arbeitsstunden

Eine Eingabe veranlasst uns, darauf hinzuweisen, dass, soweit mehrere Beschäftigte auf eine Anwendung im PC ohne individuelles Passwort zugreifen können und ihre Arbeitsstunden darüber erfassen, die protokollierten Zugriffe niemanden zugeordnet werden können. Wenn dann auch noch anlässlich der Anmeldung und Abmeldung durch Anklicken der Anwendung die Arbeitszeiten erfasst werden sollen, kann jede zugriffsberechtigte Person die Arbeitszeiten der anderen Beschäftigten manipulieren. Dieses Verfahren entspricht nicht den Anforderungen des Bundesdatenschutzgesetzes. Danach ist bei der automatisierten Verarbeitung personenbezogener Daten die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes entspricht.

Wenn mehrere Beschäftigte auf einem PC ihre Arbeitsstunden durch Anmelden und Abmelden erfassen, sind technische und organisatorische Maßnahmen zu treffen, die gewährleisten, dass nur die oder der Beschäftigte ausschließlich auf die eigenen Arbeitszeitdaten zugreifen darf. Zudem bedarf es entsprechender Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dies ist nur der Fall, wenn sich jede oder jeder Beschäftigte über ein jeweils individuelles eigenes Passwort anmeldet und abmeldet sowie nur deren oder dessen individuellen Zugangsdaten erfasst werden.

### 12.2.7 Sozialversicherungsnummer und Steueridentifikationsnummer für Werkausweise

Anlässlich einer Beschwerde möchten wir klarstellen, dass, soweit ein Werkausweis für Beschäftigte einer Firma vorgesehen ist, darin nur die Angaben der oder des Beschäftigten aufgenommen werden dürfen, die ihre beziehungsweise seine Identifizierung als Angehörige oder als Angehöriger des Unternehmens ermöglichen, beispielsweise Name, Porträtfoto, Zugehörigkeit zur Firma. Die Aufnahme der Sozialversicherungsnummer und Steueridentifikationsnummer ist für den Nachweis der Identität als Angehörige beziehungsweise als Angehöriger des Unternehmens nicht erforderlich und verstößt gegen das Bundesdatenschutzgesetz.

### 12.2.8 Anfertigung einer Kopie des Ausweises für ein Vorstellungsgespräch

Ein Bürger fragte an, ob Arbeitgeberinnen und Arbeitgeber vor Beginn eines Vorstellungsgesprächs vom vorgelegten Ausweis eine Kopie anfertigen dürfen. Wir haben dargelegt, dass Arbeitgeberinnen und Arbeitgeber nach dem Bundesdatenschutzgesetz nur die Daten erheben, speichern und nutzen dürfen, die für die Entscheidung über die Stellenbesetzung erforderlich sind.

Es reicht zur Identifizierung einer Bewerberin oder eines Bewerbers aus, wenn der Ausweis vorgelegt und damit die Identität nachgewiesen wird. Unverzüglich danach

ist der Ausweis zurückzugeben. Da durch die Anfertigung einer Kopie des Ausweises unzulässig nicht erforderliche Bewerberdaten gespeichert werden, sind Arbeitgeberinnen und Arbeitgeber verpflichtet, die Kopie unverzüglich zu vernichten. Sollte die Kopie gescannt worden sein, ist die Datei zu löschen.

Wir haben den Petenten gebeten, uns Name und Anschrift des Unternehmens zu nennen, damit wir ohne Nennung seiner Identität den Vorgang dort überprüfen können. Dies ist leider nicht geschehen.

## 13. Videoüberwachung

### 13.1 Allgemeine Einleitung

Aufgrund der außerordentlichen Intensität einer Videoüberwachung für die Beobachteten besteht für die verantwortlichen Stellen die gesetzliche Verpflichtung, nicht nur bei der Erhebung, Speicherung und Nutzung der Videoaufnahmen sorgsam und korrekt vorzugehen. Auch die Installation der Anlage sowie ihr Betrieb erfordern immer auch angemessene technische und organisatorische Maßnahmen. Deren Auswahl richtet sich nach den zu betrachtenden Risiken für das Recht auf informationelle Selbstbestimmung der Beobachteten. Für jeden Einzelfall muss die Angemessenheit und Wirksamkeit der getroffenen Maßnahmen geprüft werden, da davon auszugehen ist, dass keine Videoüberwachungsmaßnahme der anderen gleicht. Dennoch gibt es grundlegende Anforderungen, die bei jeder Videoüberwachung in Betracht zu ziehen sind und Grundlage für die zu ergreifenden Maßnahmen sein sollten. Allein die im Vorfeld festzulegende Überwachungsart hat erhebliche Auswirkungen auf die Auswahl und Ausgestaltung der Maßnahmen. Sollen die Videokameras lediglich zur Beobachtung eingesetzt werden, ohne Aufzeichnung der Bilder, sind die Anforderungen wegen der geringeren Eingriffstiefe in die Persönlichkeitsrechte der Betroffenen weniger hoch. Hingegen sind zusätzliche Maßnahmen erforderlich, wenn die Bilder für eine spätere Weiterverwendung gespeichert werden sollen. Selbst die gewählte Überwachungstechnik spielt hierbei eine Rolle. Bei den in der Vergangenheit meist verwendeten Analogkameras, die größtenteils eigenständig arbeiten, werden die Bilder direkt über ein Koaxialkabel (herkömmliches Antennenkabel) an Monitore oder Aufzeichnungsgeräte übertragen. Allerdings werden zunehmend Kameras eingesetzt, die eine direkte Einbindung der Bilder in ein Rechnernetz ermöglichen. Da diese Kameras auch mit zusätzlichen Eigenschaften ausgestattet werden können, wie zum Beispiel einem Schwenkneigekopf oder Zoomobjektiv, können sie durch ihre Fernsteuerungsmöglichkeit als Überwachungsinstrument genutzt werden. Aufgrund des erhöhten Gefährdungspotenzials dieser Technik muss die verantwortliche Stelle beim Einsatz derartiger Kameras besondere Maßnahmen ergreifen. Sie muss in jedem Fall dafür sorgen, dass zum Beispiel die Kommunikation zwischen Kamera und Videoserver verschlüsselt wird, dass das Netz rechnertechnisch abgeschottet wird sowie die relevanten Betriebsräume vor unberechtigtem Zutritt geschützt werden.

Im Rahmen unserer Vorortprüfungen haben wir oftmals festgestellt, dass der Erfassungsbereich der Kameras weit über das zur festgelegten Zweckerreichung erforderliche Maß hinausging und demzufolge auch dem Prinzip der Datenvermeidung und Datensparsamkeit widersprach. Häufig wurden so auch öffentlich zugängliche Bereiche mit erfasst, wie Straßen, Wege oder Plätze. Da die Überwachung dieser Bereiche rechtswidrig ist, muss die verantwortliche Stelle sicherstellen, dass sie ausgeblendet werden. Um dies zu erreichen, arbeitet man mit softwareseitigen Verpixelungen der erfassten Bildausschnitte oder es werden mechanische Vorrichtungen zum Abdecken des Kameraobjektives angebracht.

Wichtig ist in diesem Zusammenhang auch die revisionssichere Protokollierung der administrativen Tätigkeiten und Zugriffe auf das Videoüberwachungssystem. Eine Neuausrichtung der Erfassungsbereiche der Kameras sowie jede vergleichbare Veränderung am System, jede Authentisierung von Nutzerinnen und Nutzern und jede Einsicht und Auswertung der gespeicherten Videoaufzeichnungen müssen daher protokolliert werden.

Auch in diesem Berichtszeitraum wurde wieder eine Vielzahl von Fällen aus dem Bereich der Videoüberwachung an uns herangetragen, von denen wir nachfolgend eine Auswahl näher darstellen.

### 13.2 ECE Einkaufszentrum

Bereits im Vorjahr berichteten wir darüber, dass große Teile der Ladenpassagen der ECE Einkaufszentren mit Videokameras überwacht werden und der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit diese Angelegenheit federführend bearbeitet. Sein Ergebnis bildete die Grundlage für unsere zwischenzeitlich erfolgte Prüfung des bremischen ECE Einkaufszentrums (Roland-Center). Es wurde von uns kontrolliert, ob auch in Bremen die Absprachen zwischen der Datenschutzbehörde in Hamburg und dem Unternehmen ECE entsprechend umgesetzt und die nicht für zulässig erachteten Kameras abgebaut wurden. Im Rahmen unserer Vorortprüfung verschafften wir uns einen Eindruck von den örtlichen Begebenheiten in der Einkaufspassage und nahmen Einsicht in die Bilddaten. Hierbei stellten wir fest, dass die Kameras an den grundsätzlich für unzulässig angesehenen Standorten größtenteils abmontiert wurden. Lediglich die in den Zugangsbereichen des Centers installierten Kameras wurden nicht entfernt. Hinsichtlich dieser Videokameras konnte uns die Erforderlichkeit sowie Zweckmäßigkeit durch vorgelegte Unterlagen nachgewiesen werden. Zudem handelt es sich bei den erfassten Eingangsflächen nicht um Verweilzonen, an denen sich die Besucherinnen und Besucher aufhalten. Vielmehr handelt es sich hier um Bereiche, die von den Besucherinnen und Besuchern des Centers nur durchschritten werden, um zu den Geschäften im Center zu gelangen oder dieses wieder zu verlassen. Diese Verhaltensweise der Besucherinnen und Besucher hat sich auch bei der Einsicht in die laufenden Bilddaten bestätigt. Wir setzten durch, dass die Erfassungsbereiche der Kameras durch irreversible Schwärzungen auf das zur Zweckerreichung unbedingt Erforderliche begrenzt wurden. Bei der Vorortprüfung stellten wir fest, dass die Kamera, die zulässigerweise die Schließfächer überwachen sollte, auch die Informationstheke sowie Teilbereiche eines Geschäftes mit erfasste. Wir setzten durch, dass diese Kamera abmontiert und an einer neuen Position installiert wurde. Der Erfassungsbereich der Kamera ist nunmehr nur auf den Bereich um die Schließfächer begrenzt, wodurch nur noch die Personen erfasst werden können, die sich auch unmittelbar dort aufhalten.

### 13.3 Friseursalon

Im Berichtsjahr wurden wir darüber unterrichtet, dass in einem Friseursalon in den Umkleideräumen und Aufenthaltsräumen der Mitarbeiterinnen mehrere Videokameras installiert waren. Wir führten eine Vorortprüfung durch, um den Zweck der Videoüberwachung sowie die einzelnen Kamerastandorte und deren Erfassungsbereiche zu ermitteln.

Als Grund für die Installation der insgesamt vier Videokameras wurde uns angegeben, dass man sich gegen Einbruch und Vandalismus schützen wollte. Allein im letzten Jahr wurde zweimal eingebrochen und Waren gestohlen sowie im erheblichem Umfang das Geschäft verwüstet. Auf Nachfrage teilte man uns mit, dass die Übergriffe jedoch alle nach Geschäftsschluss verübt worden waren. Es bestand daher aus unserer Sicht keine Notwendigkeit, dass die Kameras auch während der Geschäftszeiten aktiviert sind. Aufgrund unserer Einwände wurde die Programmierung der Aktivierungszeit für die Kameras geändert, wodurch sie nur noch außerhalb der Geschäftszeiten aufzeichnen. Durch die Einsichtnahme in die aufgezeichneten Bilddaten konnten wir die von den Kameras überwachten Bereiche ermitteln. Aufgrund dieser gewonnenen Erkenntnisse wurden die Erfassungsbereiche nunmehr so angepasst, dass nur noch die Eingangstüren, die Fensterfronten sowie Warenregale erfasst werden. Des Weiteren haben wir erreicht, dass die Bilddaten nunmehr nach drei Tagen automatisch gelöscht und deutlich sichtbare Hinweisschilder auf die Videoüberwachung angebracht werden.

Außerdem wurde in der erstellten Verfahrensbeschreibung aufgenommen, dass die Videoüberwachung nur außerhalb der Geschäftszeiten durchgeführt wird. Darüber hinaus werden zukünftig bei Zugriffen auf gespeicherte Daten Protokolle geführt, aus denen ersichtlich ist, welche Personen unter welchen Voraussetzungen Einsicht in die Bilddaten genommen haben.

### 13.4 Volkshochschule Bremerhaven

Im November 2011 wurden wir auf eine Videoüberwachung in der Volkshochschule Bremerhaven hingewiesen. Es wurde vermutet, dass unter anderem der Gang zu den Personaltoiletten und Bürotüren überwacht würde. Bei einer Vorortprüfung konnten wir feststellen, dass keine Überwachung von Bürotüren oder Toilettentüren

durchgeführt wurde. Die Volkshochschule Bremerhaven teilte uns als Grund für die Installation der Kameras mit, dass in den überwachten Bereichen sehr viele Bargeldzahlungen vollzogen würden und es vor Anbringung der Videokameras mehrfach zu Überfällen auf die dort beschäftigten Mitarbeiterinnen und Mitarbeiter gekommen sei. Während der Prüfung konnten wir durch Einsichtnahme in die Bilddaten des Kassenbereichs feststellen, dass die Bezahlvorgänge von den Kameras erfasst wurden, ebenso wie der gesamte Raum, und die Arbeitsplätze der dort tätigen Mitarbeiterin und des dort tätigen Mitarbeiters. Wir erläuterten der Volkshochschule in unserem Prüfbericht, dass es im vorliegenden Fall zur Erreichung des Zwecks völlig ausreichend sei, ausschließlich den unmittelbaren Bereich, in dem der Bezahlvorgang durch den Kunden vollzogen wird, per Videokamera zu überwachen. Eine Überwachung des gesamten Raums sowie der Arbeitsplätze war nicht erforderlich. Eine weitere Kamera war in einem Flur installiert und soll die sich hier befindlichen Zugangstüren zum Kassenbereich überwachen. In diesem Fall kamen wir zu dem Ergebnis, dass der Erfassungsbereich der Kamera durch irreversible Schwärzungen auf die Zugangstüren und den unmittelbar davor befindlichen Flurbereich zu begrenzen ist. Darüber hinaus war in den Foyers der beiden vorhandenen Säle je eine Kamera montiert, deren Zweck damit begründet wurde, dass in den Sälen Veranstaltungen stattfinden und in dem überwachten Bereich Tische aufgestellt werden, um dort die Eintrittsgelder sowie Kosten für in Anspruch genommenes Catering zu kassieren. Auch in diesem Fall kamen wir zu dem Ergebnis, dass eine Überwachung der Räumlichkeiten vor den Sälen im derzeitigen Umfang rund um die Uhr nicht erforderlich war. Hier war durch technische oder organisatorische Maßnahmen sicherzustellen, dass die jeweilige Kamera nur während der Abwicklung der Bezahlvorgänge aktiviert wird.

Von der Volkshochschule Bremerhaven wurde uns die Umsetzung aller von uns in unserem Prüfbericht geforderten Maßnahmen bestätigt sowie die entsprechende Anpassung der Verfahrensbeschreibung und die zukünftige Erstellung eines Protokolls über Zugriffe auf die Videodaten.

### 13.5 Rettungsdienst

Durch einen Artikel einer Tageszeitung wurden wir darauf aufmerksam, dass die Feuerwehr in Bremerhaven zwei ihrer Rettungstransportwagen mit Videokameras ausgestattet hatte. Auf unsere Anfrage hin wurde uns mitgeteilt, dass im Außenbereich an zwei Rettungswagen je vier Kameras installiert wurden, die eine 360 Grad Rundumsicht erlauben und den unmittelbaren Bereich rund um das Fahrzeug abdecken. Die Kameras sind nur in Betrieb, wenn das Fahrzeug steht. Während der Fahrt finden keine Videoaufnahmen statt. Die Kameras wurden installiert, weil Rettungssanitäter in der Vergangenheit während ihres Einsatzes wiederholt Ziel von körperlichen Übergriffen waren, bei Rettungseinsätzen in den Fahrzeugen zur Behandlung von Notfallpatientinnen und Notfallpatienten bereit gehaltene Medikamente entwendet und die Rettungswagen beschädigt sowie Fahrzeugteile gestohlen wurden. Die Feuerwehr Bremerhaven begründete die Installation rechtlich damit, dass die Überwachung zur Wahrnehmung des Hausrechts erforderlich ist und schutzwürdige Interessen der Betroffenen nicht überwiegen. In einer von der Feuerwehr Bremerhaven vorab eingeholten Expertise wurde festgestellt, dass es im Bremischen Hilfeleistungsgesetz zwar Regelungen zur Datenverarbeitung gab, jedoch eine Datenerhebung und Datenspeicherung mittels Videokamera nicht enthalten und somit die allgemeinen Datenschutzgesetze heranzuziehen waren.

Wir teilten die Auffassung der datenschutzrechtlichen Expertise soweit sie davon ausgeht, dass das Bremische Hilfeleistungsgesetz die Videoüberwachung durch Rettungswagen nicht erlaubte. In diesem speziellen Gesetz zum Rettungsdienst gab es Regelungen zur Datenverarbeitung, aber keine Vorschriften hinsichtlich einer Datenerhebung und Datenspeicherung mittels Videokamera. Diese Regelungen des Bremischen Hilfeleistungsgesetzes waren abschließend und sperrten den Rückgriff auf das Bremische Datenschutzgesetz. Daher war keine Rechtsgrundlage ersichtlich, die im vorliegenden Fall eine Videoüberwachung erlaubte. Wir forderten zur weiteren Beurteilung der Angelegenheit detaillierte Unterlagen an und baten, bis zur abschließenden Klärung der Angelegenheit die Videoüberwachung einzustellen sowie keine weiteren Fahrzeuge mit Kameras auszustatten.

Nach Einsicht und Prüfung der uns zur Verfügung gestellten Unterlagen kamen wir zu dem Ergebnis, dass die Videoüberwachung datenschutzrechtlich unzulässig war. Aus unserer Sicht war keine Rechtsgrundlage ersichtlich, die im vorliegen-

den Fall eine Videoüberwachung durch Rettungsdienste erlauben würde. Diese Rechtsauffassung wurde von der Feuerwehr Bremerhaven nicht geteilt, die nach wie vor im Bremischen Datenschutzgesetz eine Ermächtigungsgrundlage für die Durchführung der Videoüberwachung sah.

In einer Sitzung der mit dieser Angelegenheit befassten Deputation für Inneres und Sport schloss sich der Senator für Inneres und Sport unserer Rechtsauffassung an.

Der Senator für Inneres und Sport wurde von der Innendeputation gebeten, der Bremischen Bürgerschaft einen entsprechenden Gesetzentwurf zur Änderung des Bremischen Hilfeleistungsgesetzes vorzulegen, der zum Ziel haben sollte, den Einsatz einer Videoüberwachung für Rettungswagen unter Berücksichtigung der datenschutzrechtlichen Belange zu ermöglichen. Den uns zur Stellungnahme vom Senator für Inneres und Sport übersandten Entwurf konnten wir in der vorgelegten Fassung nicht unterstützen. In unserer Antwort an die senatorische Dienststelle forderten wir unter anderem, die Videoüberwachung zumindest offen kenntlich zu machen und nur auf die Rettungstransportwagen des Rettungsdienstes zu begrenzen sowie diese nur bei Stillstand des Rettungstransportwagens im Rahmen eines Rettungseinsatzes zu aktivieren. Außerdem sollte die Speicherfrist auf 24 Stunden begrenzt werden, und die Speicherung der Bildaufzeichnungen auf solche eingeschränkt werden, die der Verfolgung von Straftaten gegen die Rettungskräfte dienen, jedoch nicht darüber hinaus auch dem Schutz der Güter des Rettungsdienstes. Unsere letztgenannte Forderung und die Forderungen, die Videoüberwachung nur auf die Rettungstransportwagen des Rettungsdienstes zu begrenzen sowie die Speicherfrist auf 24 Stunden festzulegen, wurden nicht erfüllt.

Am 24. April 2012 wurde vom Senat der Bremischen Bürgerschaft (Landtag) der Entwurf eines Gesetzes zur Änderung des Bremischen Hilfeleistungsgesetzes zur Beschlussfassung überreicht und auch beschlossen.

### 13.6 Bericht aus dem Arbeitskreis Steuerverwaltung

Die Landesbeauftragte für Datenschutz und Informationsfreiheit nahm auch in diesem Berichtsjahr an der alljährlichen Sitzung des Arbeitskreises Steuerverwaltung der Datenschutzbeauftragten des Bundes und der Länder teil. Dieser Arbeitskreis behandelte im Berichtsjahr unter anderem die folgenden Themen: Steueridentifikationsnummer, Erhebung von Kontendaten bei der SCHUFA, ElsterOnline (elektronische Steuererklärung), Steigerung der Kontendatenabfragen, Daten aus dem Kontenabrufverfahren für die Vollstreckung anderer kommunaler Forderungen, Aufbewahrung von Unterlagen nach § 147 Abgabenordnung sowie Erläuterung von Steuererstattungsbeträgen auf Überweisungsträgern der Kreditinstitute.

## 14. Dienstleistungen, Handel, Werbung und Adresshandel

### 14.1 Werbung durch eine politische Partei

Eine politische Partei hatte Namen und Adressen von Rechtsanwältinnen und Rechtsanwälten erhoben. Die Informationen hierfür stammten von der Homepage der Hanseatischen Rechtsanwaltskammer. Die Daten wurden für Zwecke der Wahlwerbung genutzt. Obwohl eine Betroffene daraufhin der Nutzung ihrer Daten für diese Zwecke widersprochen hatte, erhielt sie ein Jahr später erneut ein Werbeschreiben dieser Partei. Daraufhin forderte sie die Partei auf, ihre Daten vollständig zu löschen. Auf unsere Anfrage hin erklärte die Partei, sie könne Widersprüche nicht berücksichtigen, wenn die Daten der Betroffenen auf deren Anforderung vollständig gelöscht worden seien. Dass Personen, die sich gegen die Übersendung von Anschreiben gewendet hätten, nicht erneut angeschrieben würden, könne nur gewährleistet werden, wenn die Adressdaten der der Werbung widersprechenden Betroffenen separat gespeichert würden. Nur durch einen Abgleich der aus dem Internet erhobenen und gespeicherten Daten mit der Datei der Widersprechenden könne über einen Selektionsschlüssel gewährleistet werden, dass dieser Personenkreis keine Werbung mehr erhalte. Bei einer vollständigen Datenlöschung wäre diese Selektion nicht mehr möglich.

Nachdem die Partei um Vorschläge zu einer Lösung dieses Problems gebeten hat, schlugen wir folgendes Verfahren vor: Soweit Betroffene der Werbung widersprechen, wird ihnen wahlweise empfohlen, die vollständige Löschung ihrer Daten zu verlangen. Sie werden darauf hingewiesen, dass sie in diesem Fall damit rechnen müssten, erneut Werbung zu erhalten. Alternativ können die Betroffenen ver-

langen, dass ihre Adressdaten in einer separaten Sperrdatei gespeichert und ausschließlich zur Vermeidung von Werbeschreiben genutzt werden. Die Partei erklärte, zukünftig dieses Verfahren zu übernehmen.

Anlässlich der Überprüfung haben wir auch festgestellt, dass die Werbeschreiben keinen ausdrücklichen Hinweis auf das Widerspruchsrecht enthielten, der vom Bundesdatenschutzgesetz zwingend vorgeschrieben ist. Nach unserem Hinweis erklärte die Partei, diesen Hinweis zukünftig in alle Werbeschreiben, zu denen auch Einladungen zu politischen Veranstaltungen gehören, aufzunehmen.

### 14.2 Öffentlich zugänglicher Briefkasten für Kundenkarten im Rahmen einer Werbeaktion

In einem Einkaufszentrum wurde die Werbeaktion „Meine Kundenkarte" durchgeführt. Die ausgefüllten Anträge für Kundenkarten enthielten Name, Straße, Ort, Telefonnummer und Geburtsdatum der Teilnehmenden. Eingeworfen wurden diese Anträge in einem öffentlich zugänglichen Briefkasten mit einem relativ großen Einwurfschlitz. Da der Briefkasten bis zum Einwurfschlitz gefüllt war, konnte jede Person die ausgefüllten Anträge herausziehen. Auch war nicht erkennbar, wer für diese Werbeaktion verantwortlich war, zumal bei der Verlosung die Öffentlichkeit ausgeschlossen war.

Auf Nachfrage erklärte die Werbegemeinschaft des Einkaufszentrums, sie sei für die Aktion verantwortlich. Es sei historisch bedingt, dass auch Telefonnummer und Geburtsdatum für die Gewinnbenachrichtigungen abgefragt würden. Diese Daten würden nur für diesen Zweck verarbeitet. Bei der nächsten Gewinnspielaktion würden auf die Telefonnummer und das Geburtsdatum verzichtet.

Außerdem sei der Einwurfschlitz nunmehr durch eine von innen fest angebrachte Metallplatte reduziert worden. Künftig dürfe daher ein Eingriff in den Briefkasten und eine Entnahme von Gewinnspielkarten unmöglich sein.

### 14.3 Hinterlegung des Personalausweises als Pfand für Schließfachschlüssel in einem Einkaufszentrum

Nachdem die Geschäftsleitung eines Einkaufszentrums die Erfahrung gemacht hatte, dass ausgegebene Schlüssel zu den nur in begrenzter Anzahl zur Verfügung stehenden Kundenschließfächern oftmals nicht mehr zurückgegeben und Schließfächer dauerhaft belegt wurden, entschloss sie sich, zur Absicherung der Schlüsselrückgabe künftig den Personalausweis der Nutzerinnen und Nutzer der Schließfächer als Pfand einzubehalten.

Zwar war diese Handhabung praktisch nachvollziehbar, allerdings blieben dabei die rechtlichen Vorgaben außer Acht. Datenschutzrechtlich dürfen bei einem Vertrag, hier also über die unentgeltliche Nutzung eines Schließfachs für die Länge des Einkaufs, alle Angaben über Vertragspartnerinnen und Vertragspartner erhoben und aufbewahrt werden, die zur Vertragsdurchführung erforderlich sind. Dies sind bei Nutzerinnen und Nutzern von Schließfächern primär die üblichen Identitätsdaten, also Name und Adresse, da sie gegebenenfalls zwecks Rückgabe des Schließfachschlüssels oder etwa im Falle von Beschädigungen des Schließfachs erreichbar sein müssen. Zulässig ist es auch, eine Überprüfung der angegebenen Identitätsdaten mittels Abgleichs mit einem Personalausweis oder sonstigen amtlichen Identitätsdokumenten durchzuführen. Datenschutzrechtliche Bedenken ergeben sich aber aus der mit einer Hinterlegung an der Servicetheke einhergehenden erleichterten Möglichkeit der Kenntnisnahme weiterer für den Vertrag nicht benötigter Personalsausweisdaten durch unterschiedliche Mitarbeiterinnen beziehungsweise Mitarbeiter der Servicestelle. Die diesbezüglich bestehende Gefahr eines Missbrauchs des Identitätsdokuments oder des Zugriffs Dritter bedarf keiner weiteren Erwähnung. Hinzu kommt, dass der Gesetzgeber aufgrund der existierenden Missbrauchsgefahren, insbesondere bei einem Personalausweis der neuen Generation, im bestehenden Personalausweisgesetz sogar ein ausdrückliches Verbot aufgenommen hat, von den Inhaberinnen und Inhabern von Personalausweisen eine Hinterlegung des Ausweisdokuments zu verlangen.

Nachdem wir die Geschäftsleitung auf die datenschutzrechtlichen Bedenken sowie das bestehende personalausweisrechtliche Hinterlegungsverbot hingewiesen hatten, nahm diese umgehend Abstand von der bisherigen Vorgehensweise und führte ein alternatives datenschutzgerechtes Verfahren zur Absicherung der Schlüsselrückgabe ein.

### 14.4 Registrierungsformulare bei Hotels

Einige Anfragen erhielten wir im Berichtszeitraum zu Registrierungsformularen, die Hotelgästen bei ihrer Aufnahme in Hotels seitens der Rezeptionsmitarbeiterin beziehungsweise des Rezeptionsmitarbeiters zum Ausfüllen vorgelegt worden waren.

Nach einer Regelung des Bremischen Meldegesetzes, die sich nahezu wortgleich auch in den Meldegesetzen der anderen Bundesländer findet, sind Gäste von Hotels und anderen sogenannten Beherbergungsstätten verpflichtet, am Tag ihrer Ankunft einen besonderen Meldeschein auszufüllen und zu unterschreiben. In diesem Meldeschein muss der Gast den Tag der Ankunft und der voraussichtlichen Abreise, seinen Familiennamen, seinen (gebräuchlichen) Vornamen, sein vollständiges Geburtsdatum, seine Wohnanschrift sowie seine Staatsangehörigkeit(en) angeben. Die Leitung der Beherbergungsstätte ist verpflichtet, auf die Angabe dieser Daten hinzuwirken. Die Richtigkeit der Angaben des Gastes kann durch das Hotel gegebenenfalls durch einen Abgleich mit einem amtlichen Ausweisdokument des Gastes überprüft werden. Die Meldescheine sind bis zum Ende des dem Aufenthalt folgenden Jahres in gesicherter Weise aufzubewahren und dann zu vernichten. Die Einsichtnahme in diese Meldescheine ist ausschließlich bestimmten Behörden, insbesondere der Polizei und Staatsanwaltschaft, und nur in bestimmten Fällen, beispielsweise zur Strafverfolgung, gestattet. Die Gestaltung des Hotelmeldescheins ist durch ein amtliches Muster vorgegeben.

Mit Verwunderung nahmen wir zur Kenntnis, dass die uns vorgelegten Registrierungsformulare diesem amtlichen Muster nicht entsprachen. So wurden in den Formularen beispielsweise mehr Daten vom Gast gefordert, als sie das Melderecht vorschreibt. Gäste sollten zum Beispiel ihre Telefonnummer und E-Mail-Adresse oder das Kennzeichen ihres Kraftfahrzeuges angeben. Des Weiteren fanden sich Bestimmungen in den überprüften Registrierungsformularen, die allein die Ausgestaltung des Übernachtungsvertrages zwischen Gast und Hotel betrafen, beispielsweise Haftungserklärungen, jedoch nichts mit der gesetzlichen Meldepflicht zu tun hatten. Schließlich fehlten im Formular Hinweise darauf, dass die Angaben zu Ankunftstag und Abreisetag, Familienname und so weiter aufgrund von Vorschriften des Melderechts zwingend angegeben werden müssen.

Soweit das Melderecht die Aufzeichnung bestimmter Angaben im Hotelmeldeschein festlegt, ist deren Erhebung und Speicherung selbstverständlich auch datenschutzrechtlich zulässig. Daten jedoch, die über die melderechtlichen Vorgaben hinausgehen, können nur auf freiwilliger Basis, das heißt also mit Einwilligung des Gastes, erhoben werden. Sie sind deutlich erkennbar für den Gast als freiwillige Angaben zu kennzeichnen. Daten hingegen, die allein für das Vertragsverhältnis bedeutsam sind, haben im Meldeschein nichts verloren. Sie dienen einem anderen Zweck, nämlich der Durchführung des Vertrages, und sind deshalb dem datenschutzrechtlichen Zweckbindungsgrundsatz und Trennungsgrundsatz folgend separat zu erheben und aufzubewahren. Da das Datenschutzrecht im Übrigen festschreibt, dass über die Zwecke einer Datenerhebung und gegebenenfalls auch die zugrunde liegende Rechtsvorschrift beziehungsweise die Freiwilligkeit der Angabe zu informieren ist, waren die überprüften Registrierungsformulare auch insoweit nicht rechtskonform.

Wir haben daher die betroffenen Hotels auf die Rechtslage hingewiesen und zu entsprechenden Änderungen der Registrierungsformulare aufgefordert. Eine Anpassung wurde uns zugesagt.

### 14.5 Einsichtnahmemöglichkeit in Kassenterminals eines Unternehmens

Eine Kundin eines Handelsbetriebs berichtete uns, dass sie beim Anstehen in der Warteschlange an der Kasse in den Monitor des dortigen Kassenterminals habe Einsicht nehmen können. Während des Bezahlvorgangs des vor ihr stehenden Kunden, der offenbar Inhaber einer Kundenkarte des Unternehmens sei, habe sie auf dem Monitor eine alphabetisch geordnete Liste mit Namen und Anschriften weiterer Kunden des Unternehmens mit Kundenkarte einsehen können.

Werden personenbezogene Daten wie hier am Kassenterminal automatisiert verarbeitet, so hat die verantwortliche Stelle nach den Regelungen des Bundesdatenschutzgesetzes sicherzustellen, dass durch entsprechende technisch-organisatorische Maßnahmen ein unbefugtes Mitlesen gespeicherter Daten ausgeschlossen ist.

Nachdem wir uns die Situation vor Ort angesehen hatten und die Schilderung der Kundin bestätigt sahen, baten wir das Unternehmen, diesen Mangel abzustellen. Hierfür genügten bereits kleine organisatorische Änderungen. So wurde durch die Anbringung einer Bodenmarkierung, die nunmehr den Wartebereich anzeigt und damit für einen ausreichenden Abstand zwischen bezahlenden und nachfolgenden Kundinnen und Kunden sorgt, sowie eine Änderung der Ausrichtung des Monitors des Kassenterminals die Möglichkeit einer Einsichtnahme in die Monitoranzeige sowohl für Wartende als auch für zahlende Kundinnen und Kunden beseitigt.

### 14.6 Verkürzung des Eigenauskunftsanspruchs durch Unternehmen

Nachdem ein Betroffener eine Werbeinformation eines Unternehmens erhalten hatte, wandte er sich an das Unternehmen und forderte dieses auf, ihm darüber Auskunft zu erteilen, welche Daten über ihn gespeichert seien, woher diese stammten, an wen die Daten weitergegeben worden seien und was der Zweck der Speicherung sei. Das Unternehmen beantwortete hierauf weitestgehend alle Fragen, hinsichtlich etwaiger Empfänger der Daten außerhalb des Unternehmens selbst wies es jedoch nur darauf hin, dass bestimmte Branchendienstleister die Daten erhalten hätten. Beim Namen nannte es diese hingegen nicht. Der Betroffene wollte dies nicht auf sich beruhen lassen, weil er insoweit sein Auskunftsrecht verletzt sah, und bat uns um Nachkontrolle, ob das Unternehmen nicht konkret die Datenempfänger hätte benennen müssen und daher insoweit noch auskunftspflichtig sei.

Der Auskunftsanspruch, den der Betroffene geltend gemacht hatte und den das Bundesdatenschutzgesetz grundsätzlich allen gewährt, deren personenbezogene Daten automatisiert oder in Dateiform verarbeitet werden, schreibt dem Gesetzeswortlaut nach unter anderem vor, dass eine Auskunft zu erteilen ist „über den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden".

Auf unsere Bitte um Stellungnahme zu dieser Frage teilte uns das Unternehmen mit, dass es entsprechend der zweiten, nach dem Gesetz offenstehenden Variante ja nur zur Benennung von Empfängerkategorien verpflichtet sei.

Dies hielten wir für rechtsfehlerhaft. Zwar erweckt die vorstehend wiedergegebene Gesetzesformulierung durch das Wörtchen „oder" auf den ersten Blick den Eindruck, als habe eine auskunftspflichtige Stelle hier ein Wahlrecht hinsichtlich des Umfangs ihrer Auskunft. Nach Sinn und Zweck, Wortlaut im Zusammenspiel mit dem Kontext der Gesetzesvorschrift ist eine solche Interpretation aber nicht haltbar. Wurden Daten tatsächlich weitergegeben, so sind den Betroffenen auch die tatsächlichen Datenempfänger konkret zu benennen. Nur so ist es den Betroffenen möglich, gegebenenfalls auch gegenüber den Empfängerinnen und Empfängern der Daten, ihre unabdingbaren (vergleiche § 6 Absatz 1 Bundesdatenschutzgesetz) datenschutzrechtlichen Rechte, beispielsweise auf Löschung oder Berichtigung, durchzusetzen. Allein die Benennung von Empfängerkategorien reicht lediglich dann aus, wenn Daten im Zeitpunkt der Auskunftsanfrage tatsächlich noch nicht weitergegeben wurden, dies jedoch künftig noch beabsichtigt ist. Dies wird insbesondere auch durch den Wortlaut des einschränkenden Halbsatzes („. . ., an die Daten weitergegeben werden, . . .") klargestellt.

Das Unternehmen hielt zwar an seiner gegenteiligen Rechtsauffassung fest, erklärte sich aber bereit, im konkreten Fall auch die tatsächlichen Empfänger zu benennen und bei künftigen Auskunftsersuchen ebenfalls entsprechend unserer Rechtsauffassung zu verfahren. Es bestand daher für uns kein Anlass für weitere aufsichtsbehördliche Schritte.

## 15. Kreditwirtschaft

### 15.1 Sichtschutz an Selbstbedienungsterminals der Kreditinstitute

Der häufig unzureichende Sichtschutz bei Selbstbedienungsterminals für Kunden in den Filialen von Kreditinstituten war bereits Gegenstand der vergangenen Jahresberichte.

Bei einem Kreditinstitut hatten sich insoweit bei den Selbstbedienungsterminals in stichprobenartig kontrollierten Filialen beziehungsweise Gerätestandorten deutliche Mängel gezeigt. Trotz unserer Aufforderung zur Mängelbeseitigung verzögerte sich nach anfänglicher Aktivität an einigen Standorten gerade an weiteren, beson-

ders betroffenen Standorten die Mängelbeseitigung. Nach mehrfacher Nachkontrolle durch uns wurden aber erfreulicherweise im Berichtszeitraum auch an diesen Standorten Anstrengungen zur Verbesserung der Situation unternommen, etwa durch Umstellung und Neuausrichtung von Selbstbedienungsterminals, Aufstellen von Sichtschutzwänden, Anbringung von Bodenmarkierungen, Aufstellen von Geräten mit erschwert einsehbarem Monitor und weitere Maßnahmen. Alles in allem dürften hier nunmehr in nahezu vorbildlicher Weise Einsichtnahmemöglichkeiten für unbefugte Dritte ausgeschlossen worden sein. Weiterer aufsichtsbehördlicher Schritte bedurfte es daher nicht.

Es steht allerdings zu befürchten, dass uns bei anderen Kreditinstituten diese Thematik auch weiterhin beschäftigen wird. Erfahrungsgemäß wird oftmals viel Aufmerksamkeit auf eine moderne, offene Gestaltung von Filialräumlichkeiten oder Gerätestandorten und ein einheitliches Erscheinungsbild gelegt, dabei aber der rechtlich zu beachtende Aspekt eines ausreichenden Sichtschutzes an Selbstbedienungsterminals vernachlässigt.

## 16. Ordnungswidrigkeiten/Zwangsverfahren

### 16.1 Ordnungswidrigkeitsverfahren nach dem Bundesdatenschutzgesetz

Im Berichtsjahr wurden von uns mehrere Ordnungswidrigkeitsverfahren wegen Verstößen gegen das Bundesdatenschutzgesetz betrieben. Mehrere Verfahren betrafen erneut die Nichterteilung von Auskünften nach § 38 Absatz 3 Bundesdatenschutzgesetz an die Landesbeauftragte für Datenschutz und Informationsfreiheit als Aufsichtsbehörde. In einem der Fälle wurde von uns ein Bußgeld in Höhe von 2.000 Euro verhängt. Der Bußgeldbescheid wurde rechtskräftig und vollstreckbar, ein Vollstreckungsersuchen ist von uns an die zuständige Vollstreckungsbehörde übersandt worden.

Bereits in unserem letzten Jahresbericht (vergleiche 34. Jahresbericht, Ziffer 18.1) hatten wir berichtet, dass in mehreren Fällen, bei denen gegen die jeweiligen Bußgeldbescheide Einspruch eingelegt wurde und diesem wegen fehlender oder unzureichender Gründe nicht abgeholfen werden konnte, die Vorgänge zur weiteren Bearbeitung an die Staatsanwaltschaft Bremen abgegeben werden mussten. In einem der Fälle der von uns verhängten Bußgeldbescheide wurde das Verfahren in der Zwischenzeit mit dem Hinweis eingestellt, gegen den Beschuldigten sei bereits eine Freiheitsstrafe wegen einer von ihm begangenen Straftat verhängt worden. Bei einem der Bußgeldbescheide, mit dem ein Bußgeld in Höhe von 3.600 Euro verhängt worden war, zog die Beschuldigte ihre Eingabe auf Empfehlung des Gerichts zurück. Unser Bußgeldbescheid erlangte somit Rechtskraft, die Beschuldigte hat, wie vereinbart, die ratenweise Bezahlung der Geldbuße aufgenommen.

### 16.2 Zwangsmittelverfahren der Aufsichtsbehörde

Wie bereits in den vorhergehenden Jahren wurden im Berichtsjahr wieder Zwangsgelder angedroht und festgesetzt. Die Höhe der Zwangsgelder betrug hierbei bis zu 2.000 Euro. Gegenstand war, wie bereits in den Vorjahren, insbesondere die Nichterteilung von Auskünften durch das betroffene Unternehmen. Im Hinblick auf die Nichtergreifung notwendiger technischer und organisatorischer Maßnahmen nach dem Bundesdatenschutzgesetz und die Nichteinhaltung des Telemediengesetzes wurde in acht Fällen ein Zwangsgeld angedroht und, da die Androhung nicht zum beabsichtigten Erfolg führte, in drei Fällen auch festgesetzt.

## 17. Bericht aus dem Arbeitskreis Europa und der Arbeitsgruppe Internationaler Datenverkehr

Der Arbeitskreis „Europa“ hat sich im Berichtsjahr ausschließlich mit dem Vorschlag der Kommission „für eine Verordnung des Europäischen Parlamentes und des Rates zum Schutz personenbezogener Daten und zum freien Datenverkehr“ befasst. Diesen Entwurf hat die Kommission Ende Januar 2012 der Öffentlichkeit präsentiert (siehe auch Ziffer 1.1 dieses Berichts). Im Arbeitskreis ist dazu eine ausführliche Stellungnahme der Datenschutzbeauftragten des Bundes und der Länder sowie eine dazugehörige Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet worden (siehe auch Ziffer 18.3 dieses Berichts).

In der Arbeitsgruppe „Internationaler Datenverkehr“ wurden Fragestellungen im Zusammenhang mit verbindlichen Unternehmensregelungen – Binding Corporate

Rules (BCR) – behandelt. Hierbei handelt es sich um BCR unter deutscher Federführung und Beteiligung deutscher Aufsichtsbehörden. Des Weiteren wurde ein Verfahren der Artikel-29-Gruppe für die BCR beraten. Die Artikel-29-Gruppe ist eine Gruppe von Vertreterinnen und Vertretern datenschutzrechtlicher Aufsichtsbehörden, in der jeder Mitgliedsstaat der Europäischen Union vertreten ist. Die Gruppe hat die Aufgabe, Fragen zur Umsetzung der Datenschutzrichtlinie der Europäischen Kommission zu prüfen. Sie beschließt Vorschläge für einzelne Datenverarbeitungen. Die Vorschläge der Gruppe sollen insbesondere zur einheitlichen Anwendung der Datenschutzrichtlinie in der Europäischen Union beitragen.

Weitere Themen der Arbeitsgruppe „Internationaler Datenverkehr" waren:

— Übermittlung besonderer Arten personenbezogener Daten zum Zweck der Auftragsdatenverarbeitung in Drittstaaten mit angemessenem Datenschutzniveau,

— zuständige Aufsichtsbehörde bei der Weitergabe personenbezogener Daten von Auftragsverarbeitern in Drittstaaten mit angemessenem Datenschutzniveau an Unterauftragnehmer in Drittstaaten ohne angemessenes Datenschutzniveau,

— Orientierungshilfe Cloud Computing.

## 18. Die Entschließungen der Datenschutzkonferenzen im Jahr 2012

### 18.1 Schuldnerverzeichnis im Internet: Anzeige von Schuldnerdaten nur im Rahmen der gesetzlich legitimierten Zwecke

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. Februar 2012)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert das Bundesministerium der Justiz auf, für einen besseren Datenschutz bei der geplanten Internetabfrage aus dem Schuldnerverzeichnis Sorge zu tragen. Es sollen möglichst nur diejenigen Personen angezeigt werden, auf die sich der Abfragezweck bezieht.

Wer eine Wohnung vermieten oder einen Ratenkredit einräumen will, möchte wissen, ob sein zukünftiger Schuldner Zahlungsschwierigkeiten hat. Er hat unter bestimmten Voraussetzungen ein legitimes Interesse an der Einsicht in das von den zentralen Vollstreckungsgerichten geführte Schuldnerverzeichnis. So können sich mögliche Geschäftspartner darüber informieren, ob ihr Gegenüber in wirtschaftliche Not geraten ist.

Mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung aus dem Jahr 2009 will der Gesetzgeber die Stellung des Gläubigers stärken. Das Gesetz sieht unter anderem vor, dass der Inhalt des Schuldnerverzeichnisses ab dem 1. Januar 2013 über eine zentrale und länderübergreifende Abfrage im Internet eingesehen werden kann. Die Ausgestaltung der damit wesentlich erleichterten Einsicht wird derzeit vom Bundesministerium der Justiz durch eine Rechtsverordnung im Einzelnen vorbereitet.

Die gesetzliche Regelung erlaubt Privatpersonen die Einsicht in das Schuldnerverzeichnis nur für bestimmte Zwecke, die bei einer Anfrage darzulegen sind, zum Beispiel, um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen. Dennoch ist es derzeit vorgesehen, dass bereits nach Eingabe eines Nachnamens und des zuständigen Vollstreckungsgerichts eine Ergebnisliste mit allen Personen angezeigt wird, auf die diese beiden Kriterien zutreffen. Da Vollstreckungsgerichte jeweils zentral für ein Bundesland eingerichtet sind, erhielte die anfragende Person bei einer Vielzahl von zu erwartenden Namensgleichheiten auch Einsicht zu Angaben über Schuldner, deren Kenntnis sie zum angestrebten Zweck nicht benötigt.

Es ist zu befürchten, dass beispielsweise Vermieter Mietinteressenten nicht berücksichtigen, weil im Schuldnerverzeichnis namensgleiche Personen stehen und es ihnen zu mühsam oder zu schwierig erscheint, anhand weiterer Angaben zu prüfen, ob es sich beim Mietinteressenten tatsächlich um eine der eingetragenen Personen handelt. Auch aus der Sicht der Gläubiger ist die Anzeige von derart umfangreichen Ergebnislisten wenig hilfreich, denn um den auf die Anfrage bezogenen Datensatz aus der Liste auswählen zu können, müssen ohnehin weitere Daten wie

zum Beispiel der Vorname bekannt sein. Da es für Geschäftspartner erforderlich ist, mehr als nur den Nachnamen und den Sitz des zuständigen Vollstreckungsgerichts voneinander zu kennen, ist es auch nicht unangemessen, eine Einsicht von vornherein von weiteren Angaben abhängig zu machen.

Aus Sicht des Datenschutzes ist eine Anzeige von Schuldnerdaten, die nicht vom legitimen Abfragezweck erfasst werden, zu vermeiden. Deshalb halten es die Datenschutzbeauftragten des Bundes und der Länder für notwendig, bei der Regelung der Einsicht in das Schuldnerverzeichnis die zwingende Angabe weiterer Identifizierungsmerkmale vorzusehen.

### 18.2 Europäische Ermittlungsanordnung darf Grundrechtsgarantien nicht aushebeln

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 21. und 22. März 2012)

Zurzeit wird auf europäischer Ebene der Entwurf einer Richtlinie über die Europäische Ermittlungsanordnung in Strafsachen beraten. Diese hat massive Auswirkungen auf den Grundrechtsschutz der Bürgerinnen und Bürger in den EU-Mitgliedsstaaten (EU = Europäische Union). Sie kann dazu führen, dass der verfahrensrechtliche Schutzstandard bei strafprozessualen Maßnahmen europaweit auf niedrigstes Niveau abgesenkt wird. So kann sie etwa zur Folge haben, dass ein Mitgliedsstaat für einen anderen Daten oder Beweismittel erhebt und diesem übermittelt, obwohl die Erhebung nach eigenem Recht nicht zulässig wäre.

Der Richtlinienentwurf verfolgt vorrangig das Ziel einer weitgehenden gegenseitigen Anerkennung von Eingriffsentscheidungen der Strafverfolgungsbehörden, ohne dass einheitliche Verfahrensgarantien geschaffen werden. Dies wirft Probleme auf, wenn der Anordnungsstaat niedrigere Schutzstandards aufweist als der Vollstreckungsstaat. Die Möglichkeiten der Mitgliedsstaaten, eine entsprechende Anordnung eines anderen Mitgliedsstaates zurückzuweisen, sind nicht immer ausreichend. Eingriffsschwellen, Zweckbindungsregelungen und Verfahrensregelungen müssen gewährleisten, dass die Persönlichkeitsrechte der Betroffenen gewahrt werden.

Eine effektive grenzüberschreitende Strafverfolgung im vereinten Europa darf nicht zu Lasten des Grundrechtsschutzes der Betroffenen gehen. Die Anforderungen der EU-Grundrechtecharta sind konsequent einzuhalten. Die Europäische Ermittlungsanordnung muss in ein schlüssiges Gesamtkonzept zur Datenerhebung und Datenverwendung im Bereich der inneren Sicherheit und der Strafverfolgung eingebettet werden, das die Grundrechte der Bürgerinnen und Bürger gewährleistet.

### 18.3 Ein hohes Datenschutzniveau für ganz Europa!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 21. und 22. März 2012)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in der Europäischen Union (EU) zu modernisieren und zu harmonisieren.

Der Entwurf einer Datenschutz-Grundverordnung enthält Regelungen, die zu einer Weiterentwicklung des europäischen Datenschutzrechts führen können. Dazu gehören vor allem

— das Prinzip Datenschutz durch Technik,

— der Gedanke datenschutzfreundlicher Voreinstellungen,

— der Grundsatz der Datenübertragbarkeit,

— das Recht auf Vergessen,

— die verbesserte Transparenz durch Informationspflichten der verantwortlichen Stellen und

— die verschärften Sanktionen bei Datenschutzverstößen.

Hervorzuheben ist zudem die Geltung des europäischen Rechts für Anbieter aus Drittstaaten, deren Dienste sich auch an europäische Bürgerinnen und Bürger richten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für wesentlich, dass bei der Harmonisierung des Datenschutzrechts ein möglichst hohes Niveau für alle Mitgliedsstaaten vorgeschrieben wird. Die Konferenz hatte bereits im Konsultationsverfahren die Auffassung vertreten, dass diesem Ziel angesichts der gewachsenen Traditionen und Rechtsstandards in den Mitgliedsstaaten und der eingeschränkten begrenzten Rechtssetzungskompetenz der EU in Bezug auf innerstaatliche Datenverarbeitungsvorgänge im öffentlichen Bereich am wirksamsten durch eine Richtlinie Rechnung getragen werden kann. Wenn jetzt stattdessen der Entwurf einer unmittelbar geltenden Verordnung vorgelegt wird, muss diese im Sinne eines europäischen Mindestdatenschutzniveaus den Mitgliedsstaaten zumindest in Bezug auf die Datenverarbeitung der öffentlichen Verwaltung die Möglichkeit eröffnen, durch einzelstaatliches Recht weitergehende Regelungen zu treffen, die entsprechend der jeweiligen Rechtstradition die Grundrechte der Bürgerinnen und Bürger absichern und Raum für eine innovative Rechtsfortbildung schaffen. Nur so können beispielsweise in Deutschland die in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Datenschutzgrundsätze bewahrt und weiterentwickelt werden.

Die Konferenz erkennt an, dass die Institution der betrieblichen Datenschutzbeauftragten erstmals verbindlich in Europa eingeführt werden soll. Die Erfahrungen in Deutschland mit den betrieblichen Datenschutzbeauftragten als unabhängige Kontrollstellen und Beratungsstellen in Unternehmen sind ausgesprochen positiv. Die Konferenz bedauert deshalb, dass die Kommission grundsätzlich nur Unternehmen mit mindestens 250 Beschäftigten zur Bestellung von Datenschutzbeauftragten verpflichten will. Dieses Vorhaben bedroht eine gewachsene und erfolgreiche Kultur des betrieblichen Datenschutzes in Deutschland.

Über die bereits in dem Verordnungsentwurf vorgeschlagenen Modernisierungen hinaus hält die Konferenz weitere Schritte für erforderlich, die sie etwa in ihrem Eckpunktepapier für ein modernes Datenschutzrecht vom 18. März 2010 vorgeschlagen hat:

— eine strikte Reglementierung der Profilbildung, insbesondere deren Verbot bei Minderjährigen,

— ein effektiver Schutz von Minderjährigen, insbesondere in Bezug auf das Einwilligungserfordernis eine Anhebung der Altersgrenze,

— die Förderung des Selbstdatenschutzes,

— pauschalierte Schadenersatzansprüche bei Datenschutzverstößen,

— einfache, flexible und praxistaugliche Regelungen zum technisch-organisatorischen Datenschutz, welche vor allem die Grundsätze der Vertraulichkeit, der Integrität, der Verfügbarkeit, der Nichtverkettbarkeit, der Transparenz und der Intervenierbarkeit anerkennen und ausgestalten,

— das Recht, digital angebotene Dienste anonym oder unter Pseudonym nutzen zu können und

— die grundsätzliche Pflicht zur Löschung der angefallenen Nutzerdaten nach dem Ende des Nutzungsvorganges.

Die Regelungen zur Risikoanalyse, Vorabkontrolle und zur Zertifizierung bedürfen der weiteren Präzisierung in der Verordnung selbst.

Für besonders problematisch hält die Konferenz die vorgesehenen zahlreichen Ermächtigungen der Europäischen Kommission für delegierte Rechtsakte, die dringend auf das unbedingt erforderliche Maß zu reduzieren sind. Alle für den Grundrechtsschutz wesentlichen Regelungen müssen in der Verordnung selbst beziehungsweise durch Gesetze der Mitgliedsstaaten getroffen werden.

Die Konferenz weist darüber hinaus daraufhin, dass das im Entwurf der Datenschutz-Grundverordnung vorgesehene Kohärenzverfahren, welches die Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet, die Unabhängigkeit der Datenschutzaufsicht beeinträchtigen und zu einer Bürokratisierung des Datenschutzes führen würde. Es muss deshalb vereinfacht und praktikabler gestaltet werden.

Die durch Artikel 8 der EU-Grundrechtecharta und Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union gewährleistete Unabhängigkeit der Datenschutzaufsichtsbehörden gilt auch gegenüber der Europäischen Kommission. Die vorgesehenen Befugnisse der Kommission in Bezug auf konkrete Maßnahmen der Aufsichtsbehörden bei der Umsetzung der Verordnung wären damit nicht vereinbar.

Wiederholt hat die Konferenz auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch im **Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen** in Europa hingewiesen. Sie bedauert, dass der für diesen Bereich vorgelegte Richtlinienentwurf in vielen Einzelfragen hinter dem Entwurf für eine Datenschutz-Grundverordnung und hinter dem deutschen Datenschutzniveau zurückbleibt, etwa im Hinblick auf die Prinzipien der Datenverarbeitung (wie den Grundsatz der Erforderlichkeit) und auf die Rechte der Betroffenen (insbesondere zum Schutz des Kernbereiches der privaten Lebensgestaltung). Auch in diesem Bereich sollte die Richtlinie unter angemessener Berücksichtigung der mitgliedsstaatlichen Verfassungstraditionen ein EU-weit möglichst hohes Mindestniveau festschreiben.

Die Konferenz erklärt, dass sie den Gang des Gesetzgebungsverfahrens konstruktiv und kritisch begleiten wird.

### 18.4 Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 21. und 22. März 2012)

Mit erheblichen öffentlichen Mitteln werden derzeit zahlreiche Forschungsprojekte finanziert, die darauf abzielen, mit Hilfe modernster Technik – insbesondere der Videoüberwachung und dem Instrument der Mustererkennung – menschliche Verhaltensweisen zu analysieren. Dadurch sollen in öffentlich zugänglichen Bereichen mit hohem Sicherheitsbedarf „potenzielle Gefährder" frühzeitig entdeckt werden. Zu derartigen Forschungsvorhaben zählen beispielsweise das Projekt „INDECT" (Intelligentes Informationssystem zur Überwachung, Suche und Detektion für die Sicherheit der Bürger in urbaner Umgebung), das von der Europäischen Union gefördert wird, oder in Deutschland Projekte wie ADIS (Automatisierte Detektion interventionsbedürftiger Situationen durch Klassifizierung visueller Muster), CamInSens (Verteilte, vernetzte Kamerasysteme zur in situ-Erkennung personeninduzierter Gefahrensituationen) oder die Gesichtserkennung in Fußballstadien.

Bei der Mustererkennung soll auf Basis von Videoaufzeichnungen oder anderen Aufzeichnungen, die mit Daten aus anderen Informationsquellen kombiniert werden, das Verhalten aller erfassten Personen computerunterstützt ausgewertet werden. Menschen, deren Verhalten als ungewöhnlich eingestuft wird, können so in Verdacht geraten, zukünftig eine Straftat zu begehen. Gerade bei der Mustererkennung von menschlichem Verhalten besteht daher die große Gefahr, dass die präventive Analyse einen Anpassungsdruck erzeugt, der die Persönlichkeitsrechte der betroffenen Bürgerinnen und Bürger verletzen würde.

Insoweit ist generell die Frage aufzuwerfen, inwieweit die grundrechtliche Zulässigkeit des Einsatzes der zu erforschenden Überwachungstechnik hinreichend untersucht wird. Bei Projekten, bei denen öffentliche Stellen des Bundes und der Länder beteiligt sind, sollten jeweils die zuständigen Datenschutzbehörden frühzeitig über das Projektvorhaben informiert und ihnen Gelegenheit zur Stellungnahme eingeräumt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an alle öffentlichen Stellen von Bund und Ländern, aber auch an die der Europäischen Union, die solche Projekte in Auftrag geben oder Fördermittel hierfür zur Verfügung stellen, bereits bei der Ausschreibung oder Prüfung der Förderfähigkeit derartiger Vorhaben rechtliche und technisch-organisatorische Fragen des Datenschutzes in ihre Entscheidung mit einzubeziehen. Nur so kann verhindert werden, dass Vorhaben öffentlich gefördert werden, die gegen Datenschutzvorschriften verstoßen.

### 18.5 „Patientenrechte müssen umfassend gestärkt werden"

**Datenschutzkonferenz fordert die Bundesregierung zur Überarbeitung des vorgelegten Gesetzentwurfs auf!**

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23. Mai 2012)

Mit dem im Januar 2012 der Öffentlichkeit vorgestellten und nun dem Bundeskabinett zugeleiteten Entwurf eines Gesetzes zur Verbesserung der Rechte von Patien-

tinnen und Patienten (Patientenrechtegesetz) sollen insbesondere die bislang von den Gerichten entwickelten Grundsätze des Arzthaftungsrechts und Behandlungsrechts zusammengeführt und transparent für alle an einer Behandlung Beteiligten geregelt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder teilt das Anliegen der Bundesregierung, die Rechte von Patientinnen und Patienten zu stärken.

Die Datenschutzkonferenz hält allerdings die vorgelegten Regelungen in dem Entwurf eines Patientenrechtegesetzes für nicht ausreichend. Sie fordert die Bundesregierung nachdrücklich auf, den Gesetzentwurf zu überarbeiten und dabei die folgenden Aspekte zu berücksichtigen:

— Die vertraglichen Offenbarungsobliegenheiten der Patientinnen und Patienten gegenüber den Behandelnden dürfen nicht ausgeweitet werden. Die Patientinnen und Patienten dürfen nicht zur Offenlegung von Angaben über ihre körperliche Verfassung verpflichtet werden, die keinen Behandlungsbezug haben.

— Die Patientinnen und Patienten müssen in jedem Fall und nicht erst auf Nachfrage über erlittene Behandlungsfehler informiert werden.

— Der Gesetzentwurf sollte im Zusammenhang mit der Behandlungsdokumentation um verlässliche Vorgaben zur Absicherung des Auskunftsrechts der Patientinnen und Patienten sowie zur Archivierung und Löschung ergänzt werden.

— Der Zugang der Patientinnen und Patienten zu der sie betreffenden Behandlungsdokumentation darf nur in besonderen Ausnahmefällen eingeschränkt werden. Die in dem Entwurf vorgesehenen Beschränkungen sind zu weitgehend und unpräzise. Zudem sollte klargestellt werden, dass auch berechtigte eigene Interessen der Angehörigen einen Auskunftsanspruch begründen können.

— Der Gesetzentwurf ist um Regelungen zur Einbeziehung Dritter im Rahmen eines Behandlungsvertrages (Auftragsdatenverarbeitung) zu ergänzen.

— Regelungsbedürftig ist ferner der Umgang mit der Behandlungsdokumentation beispielsweise im Falle eines vorübergehenden Ausfalls, des Todes oder der Insolvenz des Behandelnden. Im Bereich der Heilberufe fehlt es – anders als zum Beispiel bei den Rechtsanwälten – an einem bundesweit einheitlichen Rechtsrahmen.

### 18.6 Orientierungshilfe zum datenschutzgerechten Smart Metering

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23. Mai 2012)

Intelligente Energienetze und Energiezähler sind ein zentraler Baustein zur Sicherstellung einer nachhaltigen Energieversorgung im Sinne einer ressourcenschonenden, umweltfreundlichen und effizienten Produktion, Verteilung und Nutzung von Energie. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Orientierungshilfe beschlossen, die Empfehlungen zur datenschutzgerechten Konzeption von technischen Systemen für das Smart Metering enthält. Kernstück der Orientierungshilfe ist die Beschreibung und datenschutzrechtliche Bewertung sogenannter Use Cases, das heißt Anwendungsfälle, für die einzelnen Datenverarbeitungsprozesse beim Smart Metering unter Berücksichtigung des jeweiligen Schutzbedarfs der Daten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, dass insbesondere folgende Punkte beachtet werden:

— Eine Verarbeitung der Smart Meter Daten darf nur erfolgen, soweit es für die im Energiewirtschaftsgesetz aufgezählten Zwecke erforderlich ist.

— Die Ableseintervalle müssen so groß sein, dass aus dem Verbrauch keine Rückschlüsse auf das Verhalten der Nutzer gezogen werden können.

— Smart Meter Daten sollen möglichst nur anonymisiert, pseudonymisiert oder aggregiert übermittelt werden.

— Es muss möglich sein, hoch aufgelöste Daten lokal beim Letztverbraucher abzurufen, ohne dass dieser auf eine externe Verarbeitung der Daten angewiesen ist.

— Die Daten sollen an möglichst wenige Stellen übermittelt werden.

— Es sind angemessene Löschfristen für die Daten festzulegen, um eine Vorratsdatenspeicherung zu vermeiden.

— Die Kommunikationsschritte und Verarbeitungsschritte von Smart Metering müssen zu jeder Zeit für den Letztverbraucher sichtbar und nachweisbar sein. Er muss Zugriffe auf den Smart Meter erkennen und dies im Zweifel unterbinden können.

— Zusätzlich bedarf es durchsetzbarer Ansprüche der Betroffenen auf Löschung, Berichtigung und Widerspruch.

— Der Letztverbraucher muss die Möglichkeit haben, einen Tarif zu wählen, bei dem möglichst wenig über seinen Lebensstil offenbart wird, ohne dass dies für seine Energieversorgung nachteilig ist.

— Smart Meter dürfen von außen nicht frei zugänglich sein. Es müssen eindeutige Profile für den berechtigten Zugang zu den Daten definiert werden. Anhaltspunkte hierfür bieten die Vorgaben im Schutzprofil und in der Technischen Richtlinie des Bundesamts für Sicherheit in der Informationstechnik.

— Schon bei der Konzeption und Gestaltung der technischen Systeme muss die Gewährleistung des Datenschutzes berücksichtigt werden (Privacy by Design). Der Letztverbraucher muss mit Hilfe der Technik alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten erhalten, die ihm die Kontrolle seines Energieverbrauchs und die Gestaltung seiner Privatsphäre ermöglichen, wobei der Stand der Technik nicht unterschritten werden darf. Insbesondere müssen rechtlich verbindliche Vorgaben für die Konzeption der Geräte, Verfahren und Infrastrukturen sowie für deren Einsatz geschaffen werden.

### 18.7 Melderecht datenschutzkonform gestalten!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22. August 2012)

Das vom Deutschen Bundestag am 28. Juni 2012 beschlossene neue Melderecht weist erhebliche datenschutzrechtliche Defizite auf. Schon die im Regierungsentwurf enthaltenen Datenschutzbestimmungen blieben zum Teil hinter dem bereits geltenden Recht zurück. Darüber hinaus wurde der Regierungsentwurf durch das Ergebnis der Ausschussberatungen des Bundestages noch einmal deutlich verschlechtert.

Bei den Meldedaten handelt es sich um Pflichtangaben, die die Bürgerinnen und Bürger gegenüber dem Staat machen müssen. Dies verpflichtet zu besonderer Sorgfalt bei der Verwendung, insbesondere wenn die Daten an Dritte weitergegeben werden sollen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher den Bundesrat auf, dem Gesetzentwurf nicht zuzustimmen, damit im Vermittlungsverfahren die erforderlichen datenschutzgerechten Verbesserungen erfolgen können. Dabei geht es nicht nur darum, die im Deutschen Bundestag vorgenommenen Verschlechterungen des Gesetzentwurfs der Bundesregierung rückgängig zu machen, vielmehr muss das Melderecht insgesamt datenschutzkonform ausgestaltet werden. Hierfür müssen auch die Punkte aufgegriffen werden, die von den Datenschutzbeauftragten im Gesetzgebungsverfahren gefordert worden sind, aber unberücksichtigt blieben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält insbesondere in den folgenden Punkten Korrekturen und Ergänzungen für erforderlich:

— Einfache Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels bedürfen ausnahmslos der Einwilligung des Meldepflichtigen. Dies gilt auch für die Aktualisierung solcher Daten, über die die anfragenden Stellen bereits verfügen und die Weitergabe der Daten an Adressbuchverlage. Melderegisterauskünfte in besonderen Fällen, wie Auskünfte an Parteien zu Wahlwer-

bungszwecken und an Presse oder Rundfunk über Altersjubiläen und Ehejubiläen sollten im Interesse der Betroffenen ebenfalls nur mit Einwilligung der Meldepflichtigen zulässig sein.

— Der Meldepflichtige muss sonstigen einfachen Melderegisterauskünften widersprechen können. Die Übermittlung hat bei Vorliegen eines Widerspruchs zu unterbleiben, sofern der Anfragende kein rechtliches Interesse geltend machen kann.

— Die Zweckbindung der bei Melderegisterauskünften übermittelten Daten ist zu verstärken. Die im Gesetzentwurf nur für Zwecke der Werbung und des Adresshandels vorgesehene Zweckbindung muss auch auf die Verwendung für sonstige gewerbliche Zwecke erstreckt werden.

— Angesichts der Sensibilität der Daten, die im Rahmen einer erweiterten Melderegisterauskunft mitgeteilt werden, und der relativ niedrigen Voraussetzungen, die an die Glaubhaftmachung des berechtigten Interesses gestellt werden, sollte anstelle des berechtigten Interesses ein rechtliches Interesse an der Kenntnis der einzelnen Daten vom potentiellen Datenempfänger glaubhaft gemacht werden müssen.

— Die Erteilung einfacher Melderegisterauskünfte im Wege des Abrufs über das Internet oder des sonstigen automatisierten Datenabrufs sollte wie bisher nur zulässig sein, wenn die betroffene Person ihr nicht widerspricht.

— Die Hotelmeldepflicht sollte entfallen, weil es sich dabei um eine sachlich nicht zu rechtfertigende Vorratsdatenspeicherung handelt. Hotelgäste dürfen nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen und damit in ihrem Persönlichkeitsrecht verletzt werden.

— Die erst vor wenigen Jahren abgeschaffte Mitwirkungspflicht des Wohnungsgebers bei der Anmeldung des Mieters darf nicht wieder eingeführt werden. Die Verpflichtung des Meldepflichtigen, den Vermieter zu beteiligen, basiert auf einer Misstrauensvermutung gegenüber der Person des Meldepflichtigen. Der Gesetzgeber hat die damalige Abschaffung der Vermietermeldepflicht unter anderem damit begründet, dass die Erfahrungen der meldebehördlichen Praxis zeigen, dass die Zahl der Scheinmeldungen zu vernachlässigen ist. Es liegen keine Anhaltspunkte dafür vor, dass sich dies zwischenzeitlich geändert hat. Ferner steht der Aufwand hierfür – wie auch bei der Hotelmeldepflicht – außer Verhältnis zum Nutzen.

### 18.8 Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und die GEZ rechtskonform gestalten

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. und 8. November 2012)

Die Meldebehörden sind verpflichtet, regelmäßig Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und an die Gebühreneinzugszentrale (GEZ) zu übermitteln. Die zu übermittelnden Daten beinhalten unter anderem Angaben über die Religionszugehörigkeit, aber auch Meldedaten, für die eine Auskunftssperre und Übermittlungssperre (beispielsweise wegen Gefahr für Leib und Leben oder einer Inkognito-Adoption) im Meldedatensatz eingetragen ist. Sie sind daher besonders schutzbedürftig.

Die datenschutzrechtliche Verantwortung für den rechtmäßigen Umgang mit Meldedaten tragen allein die Meldebehörden. Eine Übermittlung in elektronischer Form ist nur dann zulässig, wenn die Identitäten von Absender und Empfänger zweifelsfrei feststehen und wenn die Daten vor dem Transport verschlüsselt werden. Diese Anforderungen werden jedoch häufig missachtet.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, für die elektronische Übertragung von Meldedaten elektronische Signaturen und geeignete Verschlüsselungsverfahren mit öffentlichen Schlüsseln zu verwenden, die der jeweils aktuellen Richtlinie des Bundesamtes für die Sicherheit in der Informationstechnik entnommen sind. Durch Zertifizierung oder Beglaubigung der eingesetzten Schlüssel lassen sich auch bei der Nutzung öffentlicher Netze Absender und Empfänger eindeutig und zuverlässig identifizieren.

Mit dem Online Services Computer Interface (OSCI) steht eine bewährte Infrastruktur für E-Government-Anwendungen zur Verfügung. Die Meldeämter setzen das

Verfahren entsprechend der Bundesmeldedatenübermittlungsverordnung unter anderem für den Datenabgleich zwischen Meldebehörden verschiedener Länder ein. Wird ein auch nach heutigem Kenntnisstand sicheres Verschlüsselungsverfahren eingesetzt, ist die OSCI-Infrastruktur geeignet, die Sicherheit der Meldedatenübertragung auch an GEZ und öffentlich-rechtliche Religionsgemeinschaften zu gewährleisten. Wie jedes kryptographische Verfahren ist auch das Verfahren OSCI-Transport regelmäßig einer Revision zu unterziehen und weiterzuentwickeln.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt dem Bundesministerium des Innern, die Verwendung von OSCI-Transport für die Übermittlungen an die GEZ und die öffentlich-rechtlichen Religionsgemeinschaften vorzuschreiben und fordert die Kommunen und die Innenressorts der Länder auf, unverzüglich die gesetzlichen Vorgaben bei Datenübermittlungen an die GEZ und öffentlich-rechtliche Religionsgemeinschaften umzusetzen.

### 18.9 Europäische Datenschutzreform konstruktiv und zügig voranbringen!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. und 8. November 2012)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in Europa auf hohem Niveau zu harmonisieren. Sie hat dies bereits in ihrer Entschließung vom 21. und 22. März 2012 verdeutlicht. In zwei umfassenden Stellungnahmen vom 11. Juni 2012 haben die Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl einzelner Aspekte der Datenschutzreform bewertet und Empfehlungen für den weiteren Rechtssetzungsprozess gegeben.

Angesichts der aktuellen Diskussionen in Deutschland und im Rat der Europäischen Union sowie entsprechender Äußerungen aus der Bundesregierung im Rahmen des Reformprozesses betont die Konferenz folgende Punkte:

— Im Hinblick auf geforderte Ausnahmen für die Wirtschaft ist es für die Datenschutzbeauftragten des Bundes und der Länder unabdingbar, in der **Datenschutz-Grundverordnung** an der bisherigen Systematik des Datenschutzrechts festzuhalten. Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dies durch eine gesetzliche Grundlage oder die Einwilligung des Betroffenen legitimiert ist. Die hier für die Wirtschaft geforderten Ausnahmen lehnt die Konferenz ab. Wollte man in Zukunft nur noch eine besonders risikobehaftete Datenverarbeitung im Einzelfall regeln und die sogenannte alltägliche Datenverarbeitung weitgehend ungeregelt lassen, würde dies zu einer massiven Einschränkung des Datenschutzes führen und die Rechte der Betroffenen deutlich beschneiden.

  Jede Verarbeitung scheinbar „belangloser“ Daten kann für den Einzelnen schwerwiegende Folgen haben, wie das Bundesverfassungsgericht bereits 1983 ausdrücklich klargestellt hat. Diese Aussage gilt heute mehr denn je. Deshalb lehnt es die Konferenz ab, angeblich „belanglose“ Daten von einer Regelung auszunehmen.

  Soweit die Datenschutz-Grundverordnung eine Datenverarbeitung erlaubt, enthält der Reformvorschlag der Kommission bereits jetzt Ansätze für am Risiko der Datenverarbeitung ausgerichtete Differenzierungen. Diese sollten dort, wo ein risikobezogener Ansatz angemessen ist, weiter ausgebaut werden.

— Die Konferenz spricht sich nachdrücklich dafür aus, das bewährte Konzept eines grundsätzlich einheitlichen Datenschutzrechts sowohl für den öffentlichen als auch für den nicht öffentlichen Bereich beizubehalten und insbesondere für die Datenverarbeitung im öffentlichen Bereich die Möglichkeit eines höheren Schutzniveaus durch einzelstaatliches Recht zu belassen.

— Sie hält es für sinnvoll, für den Beschäftigtendatenschutz in der Datenschutz-Grundverordnung selbst qualifizierte Mindestanforderungen festzulegen und klarzustellen, dass die Mitgliedsstaaten über diese zugunsten des Datenschutzes hinausgehen, sie aber nicht unterschreiten dürfen.

— Mit Blick auf die **Richtlinie im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen** bekräftigt die Konferenz nochmals die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch in diesem Bereich und damit die Wichtigkeit der Verabschiedung einer entsprechenden Regelung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich im Sinne dieser Positionen im Rat der Europäischen Union für die Belange eines harmonisierten Datenschutzrechts auf einem hohen Niveau einzusetzen.

### 18.10 Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. und 8. November 2012)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist Versuche zurück, vermeintlich „überzogene" Datenschutzanforderungen für das Versagen der Sicherheitsbehörden bei der Aufdeckung und Verfolgung rechtsextremistischer Terroristen verantwortlich zu machen und neue Datenverarbeitungsbefugnisse zu begründen.

Sie fordert die Bundesregierung und die Landesregierungen auf, vor einer Reform der Struktur und Arbeitsweise der Polizeibehörden und Verfassungsschutzbehörden zunächst die Befugnisse, den Zuschnitt und die Zusammenarbeit der Verfassungsschutzbehörden vor dem Hintergrund der aufgetretenen Probleme zu evaluieren. Nur auf dieser Grundlage kann eine Diskussion über Reformen seriös geführt und ein Mehrwert für Grundrechtsschutz und Sicherheit erreicht werden.

In datenschutzrechtlicher Hinsicht geklärt werden muss insbesondere, ob die bestehenden Vorschriften in der Vergangenheit richtig angewandt, Arbeitsschwerpunkte richtig gesetzt und Ressourcen zielgerichtet verwendet worden sind. In diesem Zusammenhang ist auch zu untersuchen, ob die gesetzlichen Vorgaben den verfassungsrechtlichen Anforderungen genügen, also verhältnismäßig, hinreichend klar und bestimmt sind. Nur wenn Ursachen und Fehlentwicklungen bekannt sind, können Regierungen und Gesetzgeber die richtigen Schlüsse ziehen. Gründlichkeit geht dabei vor Schnelligkeit.

Schon jetzt haben die Sicherheitsbehörden weitreichende Befugnisse zum Informationsaustausch. Die Sicherheitsgesetze verpflichten Polizei, Nachrichtendienste und andere Behörden bereits heute zu umfassenden Datenübermittlungen. Neue Gesetze können alte Vollzugsdefizite nicht beseitigen.

Bei einer Reform der Sicherheitsbehörden sind der Grundrechtsschutz der Bürgerinnen und Bürger, das Trennungsgebot, die informationelle Gewaltenteilung im Bundesstaat und eine effiziente rechtsstaatliche Kontrolle der Nachrichtendienste zu gewährleisten. Eine effiziente Kontrolle schützt die Betroffenen und verhindert, dass Prozesse sich verselbstständigen, Gesetze übersehen und Ressourcen zulasten der Sicherheit falsch eingesetzt werden. Nur so kann das Vertrauen in die Arbeit der Sicherheitsbehörden bewahrt und gegebenenfalls wiederhergestellt werden.

Datenschutz und Sicherheit sind kein Widerspruch. Sie müssen zusammenwirken im Interesse der Bürgerinnen und Bürger.

### 18.11 Einführung von IPv6 – Hinweise für Provider im Privatkundengeschäft und Hersteller

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. und 8. November 2012)

Viele Provider werden demnächst in ihren Netzwerken die neue Version 6 des Internet-Protokolls (IPv6) einführen. Größere Unternehmen und Verwaltungen werden ihre Netze meist schrittweise an das neue Protokoll anpassen. Privatkunden werden von dieser Umstellung zuerst betroffen sein.

Für einen datenschutzgerechten Einsatz von IPv6 empfehlen die Datenschutzbeauftragten insbesondere:

— Um das zielgerichtete Verfolgen von Nutzeraktivitäten (Tracking) zu vermeiden, müssen Adresspräfixe grundsätzlich dynamisch an Endkunden vergeben werden. Auch eine Vergabe mehrerer statischer und dynamischer Adresspräfixe kann datenschutzfreundlich sein, wenn Betriebssystem und Anwendungen den Nutzer dabei unterstützen, Adressen gezielt nach der erforderlichen Lebensdauer auszuwählen.

— Entscheidet sich ein Provider für die Vergabe statischer Präfixe an Endkunden, müssen diese Präfixe auf Wunsch des Kunden gewechselt werden können. Hier-

zu müssen dem Kunden einfache Bedienmöglichkeiten am Router oder am Endgerät zur Verfügung gestellt werden.

— Privacy Extensions müssen auf Endgeräten implementiert und sollten standardmäßig eingeschaltet sein. Ist dies nicht möglich, muss eine benutzerfreundliche manuelle Wechselmöglichkeit für den Interface Identifier bestehen.

— Zusätzlich sollten die Betriebssystem-Hersteller benutzerfreundliche Konfigurationsmöglichkeiten bereitstellen, mit denen Kunden die Wechselfrequenz des Interface Identifiers auf kurze Werte festlegen können beziehungsweise einen Wechsel zu bestimmten Ereignissen anstoßen lassen können, zum Beispiel beim Start des Browsers oder beim Start oder Aufwachen des Rechners.

— Interface Identifier und Präfix sollten synchron gewechselt werden.

— Um den Ortsbezug von Adressen zu verringern, sollten Provider die Adressen für Einwahlknoten und sonstige Infrastrukturkomponenten zufällig aus dem ganzen ihnen zur Verfügung stehenden Pool auswählen und regelmäßig innerhalb des Pools wechseln.

— Damit eine sichere und vertrauenswürdige Ende-zu-Ende-Kommunikation mit IPv6 unter Nutzung des Sicherheitsprotokolls IPsec möglich ist, müssen Hersteller von Betriebssystemen starke Verschlüsselungsalgorithmen im TCP/IP-Protokollstack implementieren.

— Die Endgerätehersteller sollten ihre Produkte mit korrekt und sinnvoll vorkonfigurierten IPv6-fähigen Paketfiltern ausstatten und diese über eine leicht zu bedienende Oberfläche zugänglich machen. Bei der Aktivierung der IPv6-Unterstützung im Router sollte die Aktivierung des Paketfilters automatisch stattfinden, dem Nutzer aber zumindest empfohlen werden.

— Hersteller von nicht IPv6-fähigen Firewalls (Firmware und Systemsoftware) sollten entsprechende Updates anbieten. Hersteller von IPv6-fähigen Firewalls sollten den Reifegrad ihrer Produkte regelmäßig prüfen und soweit erforderlich verbessern.

— IPv6-Adressen sind ebenso wie IPv4-Adressen personenbezogene Daten. Sofern eine Speicherung der Adressen über das Ende der Erbringung des Dienstes hinaus unzulässig ist, dürfen Provider und Diensteanbieter IPv6-Adressen allenfalls nach einer Anonymisierung speichern und verarbeiten. Ebenso ist die Ermittlung des ungefähren Standorts eines Endgerätes anhand der IPv6-Adresse für Provider und Diensteanbieter nur nach Anonymisierung der Adresse zulässig. Zur wirkungsvollen Anonymisierung der IPv6-Adressen sollten nach derzeitigem Kenntnisstand mindestens die unteren 88 Bit jeder Adresse gelöscht werden, das heißt der gesamte Interface Identifier sowie 24 Bit des Präfix.

— Der gemeinsame Betrieb von IPv6 und IPv4 auf einem Gerät (Dual-Stack-Betrieb) führt zu erhöhtem Gefahrenpotenzial und sollte daher vermieden werden. Dies gilt auch für die als Übergangslösung gedachten Tunnelprotokolle.

— Bestimmte Arten von Anonymisierungsdiensten sind dazu geeignet, die IP-Adressen von Nutzern wirksam zu verbergen. Auch Peer-to-Peer-Anwendungen können zu einem robusten und datenschutzfreundlichen, weil nicht an einzelnen Punkten störbaren und überwachbaren Internet beitragen. Netzbetreiber können die Forschung auf diesem Gebiet unterstützen und selbst Anonymisierungsdienste anbieten. Die Verwendung von Anonymisierungsdiensten und Peer-to-Peer-Anwendungen darf durch Netzbetreiber nicht blockiert werden.

Mit der Orientierungshilfe „Datenschutz bei IPv6 – Hinweise für Hersteller und Provider im Privatkundengeschäft“ präzisieren die Datenschutzbeauftragten des Bundes und der Länder ihre Hinweise vom September 2011.

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

### 19.1 Einwilligungserklärung und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 17. Januar 2012 in Düsseldorf)

Der Düsseldorfer Kreis hat sich dafür eingesetzt, die Einwilligungserklärungen und Schweigepflichtentbindungserklärungen in der Versicherungswirtschaft transpa-

renter zu gestalten. Gemeinsam mit dem Gesamtverband der deutschen Versicherungswirtschaft e. V. haben die Datenschutzaufsichtsbehörden eine Mustererklärung erarbeitet. Die Versicherungsunternehmen sind aufgefordert, die bisherigen Einwilligungstexte zeitnah durch neue zu ersetzen, die der Mustererklärung entsprechen. Sie können den umfangreichen Text des Beschlusses im Internet unter: https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2012/EE_Versicherungswirtschaft/EE_Versicherungswirtschaft.pdf finden.

### 19.2 Near Field Communication (NFC) bei Geldkarten

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 18. und 19. September 2012 in Düsseldorf)

Es ist datenschutzrechtlich problematisch, wenn beim Einsatz von Near Field Communication (abgekürzt NFC; deutsch Nahfeldkommunikation) bei Geldkarten eine eindeutige Kartennummer, Geldbeträge und Transaktionshistorien unverschlüsselt von unberechtigten Dritten auslesbar sind. Die Geldkartenanbieter haben gemäß § 9 Bundesdatenschutzgesetz (BDSG) im Rahmen der Verhältnismäßigkeit mit angemessenen technisch-organisatorischen Maßnahmen dafür zu sorgen, dass Dritten kein unberechtigtes Auslesen von Daten möglich wird.

Datenschutzrechtlich erstrebenswert ist die Einräumung einer Wahlmöglichkeit für die Betroffenen, ob sie eine Geldkarte mit NFC-Funktionalität einsetzen wollen. Insoweit nehmen die Aufsichtsbehörden die Ankündigung der Deutschen Kreditwirtschaft zur Kenntnis, das Kartenbetriebssystem so bald wie möglich so zu ändern, dass die Betroffenen die NFC-Funktionalität einschalten und ausschalten können. Die Gefahr des (unbemerkten) unberechtigten Auslesens der Transaktionsdaten durch Dritte kann auch dadurch verringert werden, dass insofern nur das kontaktbehaftete Auslesen der Daten zugelassen wird.

Zudem sind die Vorgaben des § 6 c BDSG zu beachten. Die Betroffenen müssen ausreichend informiert werden, insbesondere über die Funktionsweise des Mediums, die per NFC auslesbaren Daten, die Schutzmöglichkeiten für die Daten und ihre Rechte als Betroffene nach den §§ 34 und 35 BDSG.

## 20. Die Europäische und die Internationale Datenschutzkonferenz

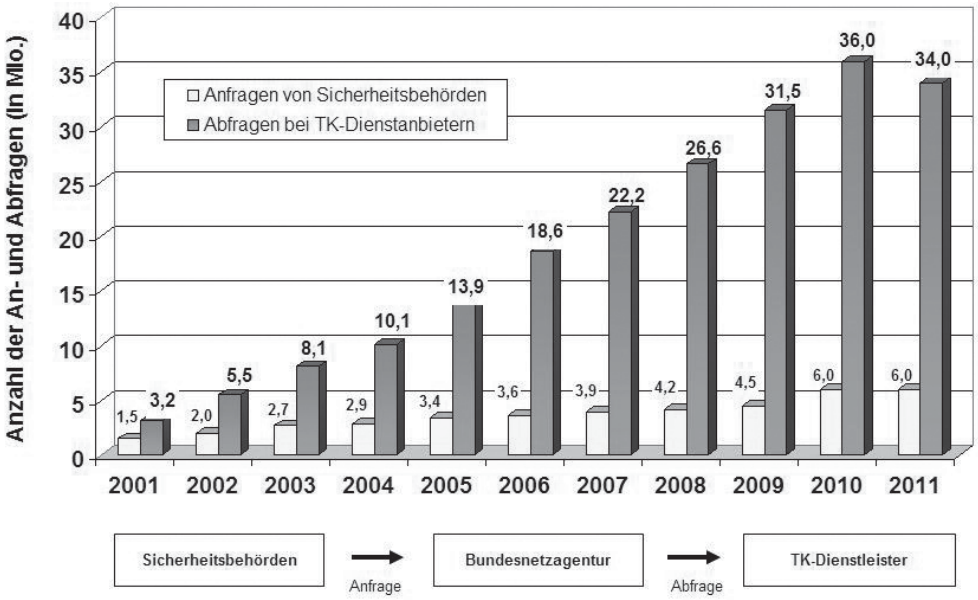
Die Entschließung der Europäischen Datenschutzkonferenz im Jahr 2012 zur europäischen Datenschutzreform steht auf der Seite des Virtuellen Datenschutzbüros in englischer Sprache unter http://www.datenschutz.de/news/detail/?nid=5358 zur Verfügung.

Informationen zu den Entschließungen der Internationalen Datenschutzkonferenz sind unter
http://www.bfdi.bund.de/DE/Entschliessungen/IntDSK/IntDSK_node.html
zu finden.

## 21. Anhang

### 21.1 Automatisiertes Auskunftsverfahren gemäß § 112 Telekommunikationsgesetz

Sicherheitsbehörden erhalten gemäß § 112 Telekommunikationsgesetz (TKG) über die Bundesnetzagentur von Telekommunikationsdiensteanbietern Auskünfte aus deren Kundendateien (Namen und Anschriften der Inhaber von Rufnummern). Rund 250 bei der Bundesnetzagentur registrierte Behörden können zurzeit bei 140 Telekommunikationsunternehmen entsprechende Bestandsdaten abrufen. Die Anzahl der Anfragen blieb im Vergleich zum Vorjahr auf gleichem Niveau.




Quelle: Jahresbericht 2011 der Bundesnetzagentur

## 21.2 Liste des verfügbaren Informationsmaterials

Informationen zu verschiedenen Bereichen können im Internet unter www.datenschutz.bremen.de abgerufen werden; hier können auch Formulare heruntergeladen werden.

## 21.3 Index

Druck: Anker-Druck Bremen