BREMISCHE BÜRGERSCHAFT **Drucksache 17 / 1708**
Landtag 25. 03. 11
17. Wahlperiode

33. Jahresbericht der Landesbeauftragten für Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats über das Ergebnis der Tätigkeit im Jahr 2010 den 33. Jahresbericht zum 31. März 2011 (§ 33 Absatz 1 Bremisches Datenschutzgesetz – BremDSG). Redaktionsschluss für die Beiträge war der 31. Dezember 2010.

Dr. Imke Sommer
Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Inhaltsverzeichnis

1. Einleitung

Das Recht auf informationelle Selbstbestimmung stand im Berichtsjahr 2010 im Blickfeld einer Reihe von politischen Debatten. Wir haben über das Ob und das Wie der Internetveröffentlichung von Ansichten der von uns bewohnten Häuser, über den Schutz der Beschäftigten vor übermäßiger Kontrolle und über die Befugnisse des Staates, unsere Kommunikation zu kennen, diskutiert. Wir haben uns darüber unterhalten, wie nicht nur Kinder und Jugendliche, sondern auch wir Älteren lernen können, uns selbst im Internet davor zu schützen, dass andere sich über unseren Willen hinwegsetzen, und was wir tun müssen, um auch selbst die durch die Würde der anderen gezogenen Grenzen zu respektieren. Was immer das konkrete Thema war, immer haben wir darüber diskutiert, wie weit Menschen über sich und das, was andere über sie wissen und sagen, selbst sollen bestimmen dürfen. Dass es diese Debatten gegeben hat, scheint dafür zu sprechen, dass 2010 ein gutes Jahr für das Grundrecht auf informationelle Selbstbestimmung war. Leider haben die öffentlichen Diskussionen aber in keinem Fall eine gesetzliche Regelung hervorgebracht, die die informationelle Selbstbestimmung der Menschen wirksam zu schützen vermag. Dies erstaunt besonders deshalb, weil in zwei Fällen entsprechende Gesetzesinitiativen mit eindeutiger Mehrheit den Bundesrat passiert haben. Der Frage, warum sich die öffentlichen Debatten nach Zwischenhochs am Ende doch so ungünstig für die informationelle Selbstbestimmung entwickelt haben, soll in den ersten drei Teilen der Einleitung nachgegangen werden. Der vierte Teil stellt die Vorschläge der Datenschutzbeauftragten des Bundes und der Länder für gesetzliche Regelungen vor, die die Grundrechte auf informationelle Selbstbestimmung und auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erfolgreich gegen Eingriffe schützen könnten. Der letzte Teil beschäftigt sich mit der Medienkompetenz als derjenigen Fähigkeit der Menschen, den Freiheitsraum, den die beiden Grundrechte bieten, in einer Weise zu nutzen, die die eigenen Rechte und die Rechte anderer respektiert.

1.1 Google Street View – oder: Wie starke Wellen vom flachen Deich gebrochen werden

Wir alle haben im letzten Jahr an einer mächtigen kollektiven Ausübung des Grundrechts auf informationelle Selbstbestimmung mitgewirkt. Es gab ein paar Wochen, da haben wir uns alle die Frage gestellt, ob wir es unschädlich finden, dass das Haus, in dem wir wohnen, weltweit im Internet zu sehen ist, ob wir es vielleicht sogar begrüßen, oder ob wir es ablehnen und das Haus unkenntlich machen (= „verpixeln“) lassen wollen. Überall wurde darüber gestritten, ob die Verpixelung als richtig oder wichtig, spießig oder spaßig anzusehen sei. Wie auch immer die individuelle Antwort auf diese Frage lautete, wo auch immer die Gründe für die Entscheidung lagen, jedes Mal machten wir von unserem Grundrecht Gebrauch, selbst darüber zu bestimmen, wer was wann über uns, in diesem Fall über die Art, wie wir wohnen, weiß.

Der Streit entbrannte dabei immer darüber, ob es richtig oder falsch ist, von dem Recht Gebrauch zu machen, vor Veröffentlichung des Dienstes Google Street View der Veröffentlichung des von uns bewohnten Hauses zu widersprechen. Dass jede und jeder von uns ein solches Vorabwiderspruchsrecht hat, und dass es ein Einzelfall bleiben muss, dass dieses Recht uns „freiwillig“ zugestanden wird, anstatt sich unmissverständlich aus dem Gesetz zu ergeben, haben in der laut tobenden öffentlichen Debatte die wenigsten falsch gefunden. Es waren im Gegenteil sogar Stimmen zu hören, die meinten, dass für das Fotografieren von Häusern zu kommerziellen Zwecken sogar eine vorherige Einwilligung der Bewohnerinnen und Bewohner erforderlich gewesen wäre.

Aber dann ist alles ganz anders gekommen: Der Bundesinnenminister hat ein allgemeines Widerspruchsrecht für unnötig erklärt. Er hat es überhaupt abgelehnt, für diesen Bereich gesetzliche Regelungen vorzuschlagen und sich dafür ausgesprochen, dass die von den Veröffentlichungen wirtschaftlich Profitierenden sich dafür selbst die Regeln geben. Die daraufhin geschaffenen Selbstregulierungsregeln der Geodatenwirtschaft sehen keinen Vorabwiderspruch vor. Die öffentliche Empörung darüber bleibt aus.

Wie ist das möglich? Was ist passiert? Wie kann der Vorabwiderspruch, mit dem wir uns alle wochenlang beschäftigt haben, plötzlich so unbedeutend werden? Hauke Haien ist in der Geschichte vom Schimmelreiter mit der Idee erfolgreich,

Deiche zum Meer hin flach anzulegen, damit sich Sturmwellen dort „totlaufen“. Die Chronologie der Ereignisse um Google Street View im Berichtsjahr 2010 scheint ein Beispiel dafür zu sein, dass dieser Mechanismus gelegentlich auch auf Wellen des öffentlichen Interesses angewendet wird.

1.1.1 Anrollen

Google Street View ist ein Internetdienst, der Straßenansichten zeigt, die wegen ihrer hohen Auflösung detaillierte Blicke auf Menschen, Autos und Häuser ermöglichen. Schon im Vorfeld hatte Google zugesichert, menschliche Gesichter und Autokennzeichen vor Veröffentlichung zu verpixeln. Die Kamera-Autos waren 2008 mit im Vergleich zu der Situation 2010 nur geringer öffentlicher Aufmerksamkeit und Empörung durch Deutschland, auch durch Bremen, gefahren und hatten 360-Grad-Aufnahmen gemacht. Wie sich später herausstellte, waren bei dieser Gelegenheit auch Daten über drahtlose Netze (WLAN) und deren Inhaltsdaten gespeichert worden.

Der Dienst Google Street View greift wie alle vergleichbaren Dienste anderer Anbieter wegen der zeitlichen und örtlichen Allgegenwärtigkeit des Internet und der beliebigen und unendlichen Verknüpfbarkeit der Google Street-View-Daten mit allen anderen vorhandenen Daten in das Grundrecht auf informationelle Selbstbestimmung ein. Datenschützerinnen und Datenschützer vertraten und vertreten den Standpunkt, dass diejenigen, die mit der Veröffentlichung einer Ansicht des von ihnen bewohnten Hauses nicht einverstanden sind, bereits nach der geltenden Rechtslage dagegen zumindest ein Widerspruchsrecht haben. Die Firma Google stützte sich auf ein Rechtsgutachten, das vom Gegenteil ausging.

Mein für Google Deutschland zuständiger Hamburger Kollege, Prof. Dr. Johannes Caspar, hatte Google Deutschland in zähen Verhandlungen 13 Zusagen abgerungen. Eine davon war die verbindliche Zusicherung, Widersprüche gegen die Veröffentlichung von Personen, Kraftfahrzeugkennzeichen, Gebäuden und Grundstücken bereits vor der Veröffentlichung zu berücksichtigen, indem die entsprechenden Bilder unkenntlich gemacht würden. Auch nach Veröffentlichung sollen Widersprüche umgesetzt werden. Gleichzeitig wurde zugesagt, Rohdaten, auf die sich Widersprüche beziehen, zu löschen.

In den Verhandlungen zur Umsetzung der zugesagten Vorabwiderspruchslösung, die Vertreterinnen und Vertreter der versammelten datenschutzrechtlichen Aufsichtsbehörden mit Google Deutschland führten, zeigte sich das nicht überraschende Phänomen, dass die Vertreterinnen und Vertreter der Firma Google in der Logik von Softwareprogrammen denken. Sie konnten sich allenfalls vorstellen, das umzusetzen, was in einer Internetanwendung abbildbar ist, die sie zwischenzeitlich entwickelten. Die Vorstellung, mit einer Internetanwendung ein ausreichendes Instrument zur Umsetzung des Vorabwiderspruchsrechts zur Verfügung zu stellen, entsprach nicht der Realität. Gerade Menschen, die keinen Internetzugang haben, wollten ihr Haus nicht in diesem Medium abgebildet sehen. In den Verhandlungen gelang es, Google Deutschland davon zu überzeugen, dass auch schriftlich eingehende Widersprüche bearbeitet werden müssen. Die Verhandlungen waren sehr stark davon geprägt, dass die Firma Google Incorporated mit Sitz in den Vereinigten Staaten von Amerika es nicht für ihre Rechtspflicht hält, uns die Vorabwiderspruchsmöglichkeit einzuräumen, sondern sie uns „freiwillig“ eröffnet hat. Der Vertreter von Google Deutschland verließ die Verhandlungen mit einer langen Liste von Fragen, deren Beantwortung durch die Firma Google, zum großen Teil durch die Google Incorporated, noch ausstand. Darunter befand sich beispielsweise die Frage, ob Google die Daten der Widersprechenden einer Treuhänderin oder einem Treuhänder überlassen würde, der oder die sie nur im Falle von Rechtsstreitigkeiten an Google ausgehändigt hätte.

Da die Beantwortung dieser Fragen noch ausstand, kam für uns die Ankündigung der Firma Google, das Internetwerkzeug für den digitalen Widerspruch werde demnächst online gestellt, sehr überraschend. Für Ärger sorgte auch die Ankündigung, der digitale Widerspruch sei vier Wochen lang, bis zum 15. September 2010, möglich. Danach eingehende Widersprüche würden nicht mehr vor Veröffentlichung des Dienstes berücksichtigt. Zu diesem Zeitpunkt war insbesondere die Frage des Verbleibs der Widerspruchsdaten noch ungeklärt. Diejenigen, die gegen die Veröffentlichung des von ihnen bewohnten Hauses widersprechen wollten, mussten sich unter Nennung ihres Namens und ihrer Adresse Google gegenüber als

Bewohnerinnen und Bewohner eines bestimmten Hauses offenbaren. Auf diese Weise erlangte das Unternehmen zusätzliche Daten, die es mit der Straßenansicht hätte verknüpfen können. Es war mehr als verständlich, dass diejenigen, die – möglicherweise aus einem Grundmisstrauen gegen die Firma Google – vorab der Veröffentlichung von Abbildungen widersprechen wollten, zunächst wissen wollten, wie die Google Incorporated mit ihren Widerspruchsdaten verfahren würde.

1.1.2 Auftürmen

Im Sommer erhob sich eine riesige Welle des öffentlichen Interesses an diesem Thema. Die gesellschaftliche Auseinandersetzung darüber, ob von dem Vorabwiderspruchsrecht Gebrauch gemacht werden sollte oder nicht, tobte. Viele wiesen darauf hin, dass Voraussetzung der Diskussion war, dass die Menschen überhaupt eine solche Entscheidungsmöglichkeit hatten, und dass diese im Fall von Google Street View nur „von Googles Gnaden" gewährt worden war. Daher reifte die Erkenntnis, dass es wichtig ist, diese Entscheidungsmöglichkeit der Menschen über die Ausübung ihres Vorabwiderspruchsrechts klarstellend im Bundesdatenschutzgesetz zu regeln. Selbst im Handelsblatt wurde das Fehlen eines klaren Gesetzes beklagt. Die verbraucherschutzpolitischen Sprecher der Regierungsfraktionen kündigten dementsprechend gesetzliche Regelungen an.

Auf dem Höhepunkt der gesellschaftlichen Aufmerksamkeit geschah zweierlei: Die Firma Google reagierte sehr defensiv und die Länder beschlossen im Bundesrat mit eindeutiger Mehrheit einen Gesetzentwurf.

Die Google Incorporated ließ Ermittlungen, die die hamburgische Staatsanwaltschaft wegen des Mitscannens der WLAN (drahtloses lokales Netzwerk) inklusive von Inhaltsdaten aufgenommen hatte, stillschweigend über sich ergehen. Auf die aufbrandende Kritik an der kurzen Frist, die Google für die Vorabwidersprüche eingeräumt hatte, reagierte die Firma mit einer Verdoppelung der eingeräumten Vorabwiderspruchsfrist von vier auf acht Wochen. Großer öffentlicher Kritik begegnete auch der schon erwähnte Umstand, dass diejenigen, die Widerspruch einlegen wollten, nicht sicher sein konnten, was Google mit ihren Widerspruchsdaten machen würde. Erst zwei Tage, nachdem das digitale Widerspruchtool online gestellt worden war, machte Google dazu eine weitere Zusage. Die Widerspruchsdaten würden sicher verwahrt, ausschließlich für das Widerspruchsverfahren verwendet und „im Rahmen der gesetzlichen Verjährung etwaiger Ansprüche" gelöscht.

Schon mehrere Wochen vor Freischaltung des Onlinewiderspruchs durch Google hatte der Bundesrat auf die Problematik reagiert, dass die Zusagen Googles aller Voraussicht nach nicht gerichtlich durchsetzbar und jedenfalls nicht für andere Geodatenanbieter, die längst ähnliche Dienste wie Street View planten oder bereits im Internet veröffentlicht hatten, bindend sind. Der mit eindeutiger Mehrheit am 9. Juli 2010 im Bundesrat verabschiedete Gesetzentwurf enthielt im Wesentlichen die gesetzliche Festschreibung derjenigen Zusagen, die die Firma Google zum Street-View-Dienst gemacht hatte. Der Entwurf wäre eine gute Grundlage für die Diskussion in Politik und Gesellschaft gewesen. Aus datenschutzrechtlicher Sicht hätte sie um die Frage der Einrichtung eines Widerspruchsregisters erweitert werden können. In einem solchen zentralen Widerspruchsregister, das von einer neutralen, nicht der Wirtschaft zuzurechnenden Stelle betrieben werden müsste, könnte sich jede und jeder einmalig mit Wirkung für alle denkbaren Fälle gegen die Veröffentlichung persönlicher Daten im Internet aussprechen. Am 13. August 2010, also fast sechs Wochen später und wenige Tage vor Freischaltung des Widerspruchstools, ließ die Bundesregierung verlautbaren, sie wolle „schon in der folgenden Woche" über die Forderung des Bundesrats nach schärferen gesetzlichen Regelungen für die Datenerfassung zu Panoramaaufnahmen im Internet und ein gesetzlich verbürgtes Widerspruchsrecht für Betroffene beraten.

Es hätte also alles so gut ausgehen können für die informationelle Selbstbestimmung, warum kam es dann nicht dazu? Wir kommen zum Stadium des Totlaufens der öffentlichen Diskussion an dem nicht enden wollenden, flach ansteigenden Deich der administrativen Reaktion und an den nicht nachlassenden bohrenden Interventionen der Lobby der Geodatenwirtschaft. So hatte Google nach Bekanntwerden der Bundesratsinitiative zur Änderung des Bundesdatenschutzgesetzes an unzählige Stellen Schreiben versandt, in denen der Gesetzentwurf als „weder notwendig noch zielführend" und als „Gefahr für die gesamte Geodatenbranche" ab-

gelehnt wurde. Die Angeschriebenen wurden gebeten, vor einer Zustimmung zu dem Gesetzentwurf dessen Nutzen mit den drastisch geschilderten Risiken „sorgfältig“ abzuwägen.

1.1.3 Totlaufen

Nach der angekündigten Kabinettssitzung teilte die Bundesregierung mit, dass sie dem Gesetzentwurf des Bundesrats nicht folgen wolle. Die Problematik solle zunächst geprüft werden. Der Bundesinnenminister wurde damit zitiert, er „sei nicht grundsätzlich gegen eine gesetzliche Regelung“ des Umgangs mit Geodaten-Diensten, wolle allerdings vor einer Entscheidung ein Spitzengespräch abwarten. Dazu wolle er für den 20. September 2010 „Vertreter von Internet-Konzernen sowie Daten- und Verbraucherschützer und Experten aus den Bundesministerien“ einladen.

In den folgenden Wochen ebbte das öffentliche Interesse am Thema ab.

Am Spitzengespräch „Digitalisierung von Stadt und Land“ nahmen neben Wissenschaftlern, Verwaltungsangehörigen, Bundestagsabgeordneten, Medienvertreterinnen und Medienvertretern 14 Unternehmensvertreterinnen und Unternehmensvertreter, der Bundesbeauftragte und zwei Landesbeauftragte für Datenschutz, ein Vertreter des Bundes der Verbraucherzentralen, ein Mieter- und ein Vermietervertreter teil.

Schon zu Beginn der Veranstaltung lag ein Eckpunktepapier des Bundesinnenministers vor, in dem er an die Geodatendiensteanbieter appellierte, nicht danach zu streben, „den gesetzlichen Rahmen stets zugunsten ihres Geschäfts auszuschöpfen“, weil sie dadurch zu gesetzgeberischen Handeln aufforderten, „unter dem die Offenheit für Innovationen letztlich“ leide. Folgerichtig zu dieser geringschätzenden Beurteilung der vom demokratischen Gesetzgeber erlassenen Gesetze, die aus dem Munde des auch für die Verfassung zuständigen Ministers erstaunt, forderte er von der Geodatenwirtschaft als Selbstregulierung die Formulierung von „übergreifenden Regeln im Sinne eines Datenschutz-Kodex“. Zu den inhaltlichen Vorgaben, die er hierfür machte, gehörte, dass die von Google im Zusammenhang mit Google Street View gemachten Zugeständnisse eines allgemeinen Vorabwiderspruchsrechts nicht wiederholt würden. „Bei der alleinigen Abbildung von öffentlich sichtbaren Häusern“ lasse sich „pauschal kein berechtigtes Interesse an einem Widerspruch oder einer Löschung bejahen“.

244 237 Menschen sahen das erklärtermaßen anders. Sie hatten nach Angaben Googles Widerspruch gegen die Veröffentlichung der von ihnen bewohnten Häuser eingelegt. Google relativierte die Zahl der Vorabwidersprüche. In den 20 Städten seien es nur 2,89 Prozent der Haushalte gewesen, die vom Vorabwiderspruchsrecht Gebrauch gemacht hätten. Mein Hamburger Kollege vermutet allerdings, dass dies hochgerechnet auf das gesamte Bundesgebiet immerhin bedeutet, dass sich deutlich über eine Million Haushalte gegen die Veröffentlichung der von ihnen bewohnten Gebäude wendet. Nach Aussage von Google Deutschland waren ein Drittel der Widersprüche schriftlich erhoben worden.

Am 18. November 2010 stellte die Google Incorporated den Dienst Google Street View für die 20 größten deutschen Städte, unter ihnen Bremen, online.

Anfang Dezember legte der Bundesinnenminister unter der Überschrift „Datenschutz im Internet“ einen Gesetzentwurf „zum Schutz vor besonders schweren Eingriffen in das Persönlichkeitsrecht“ vor. Darin machte er deutlich, dass seiner Auffassung nach nur eine solche Veröffentlichung in Telemedien unzulässig ist, die in besonders schwerer Weise in das Persönlichkeitsrecht der Betroffenen eingreift. Eine gesetzliche Regelung hält der Bundesinnenminister nun doch nur für diesen Fall für erforderlich. Alle unterhalb dieser Schwelle liegenden Eingriffe in das Persönlichkeitsrecht hält er einer gesetzlichen Regelung nicht für würdig. Der Entwurf schützt das Persönlichkeitsrecht allerdings nicht gegen alle besonders schweren Eingriffe. Besonders schwere Eingriffe in das Persönlichkeitsrecht sollen ausnahmslos dann erlaubt sein, wenn eine Rechtsvorschrift dies erlaubt (welche verfassungsmäßige Rechtsvorschrift könnte besonders schwere Eingriffe in das Persönlichkeitsrecht erlauben?), wenn die oder der Betroffene ausdrücklich und gesondert eingewilligt hat (welche Einwilligung in eine besonders schwere Persönlichkeitsverletzung könnte wirklich auf einer Willensbildung beruhen, die den datenschutzrechtlichen Anforderungen an Freiwilligkeit, Informiertheit, Widerruflichkeit und Schriftlichkeit genügt?), oder wenn ein überwiegendes schutzwürdiges Interesse

an der Veröffentlichung besteht (welches könnte das sein?). Dass die im Papier genannten Interessen der Meinungs-, Forschungs- und Pressefreiheit besonders schwere Persönlichkeitsverletzungen zu rechtfertigen vermögen, erscheint auf den ersten Blick nicht plausibel. Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

Nach der Logik seines Eckpunktepapiers sieht der Bundesinnenminister also die „rote Linie" für ein gesetzliches Regelungsbedürfnis noch nicht einmal bei besonders schweren Eingriffen in das Persönlichkeitsrecht für überschritten an. Hinzukommen müssen noch weitere Faktoren, die den Eingriff weiter in Richtung des Kernbereichs des Persönlichkeitsrechts treiben. Die Rote-Linie-Rhetorik selbst zeigt ein Grundrechtsverständnis, wonach Gesetze nur dazu dienen, den Bereich der rechts- und gesetzfreien Räume der Freiheit derjenigen, die in Grundrechte eingreifen, zu begrenzen. Bis diese späte Schwelle erreicht ist, ist jeder Grundrechtseingriff erlaubt. Dahingegen gehen wichtige Verfassungsrechtlerinnen und Verfassungsrechtler davon aus, dass der Gesetzgeber den Freiheitsraum der Grundrechte ausgestalten muss und so „praktische Konkordanz" (Begriff von Prof. Dr. Konrad Hesse) zwischen den kollidierenden Grundrechten herstellen muss. Wenn der Innenminister gerade für den Bereich des Internet ein modernes Internetdatenschutzrecht fordert, vertritt übrigens auch er diese Auffassung.

Auf der gleichen Veranstaltung, auf der der Bundesinnenminister sein Eckpunktepapier veröffentlichte, stellte die Geodatenwirtschaft einen „Datenschutz-Kodex" für Geodatendienste vor. Durch Unterwerfung unter diesen Kodex sollen Geodiensteanbieter zusichern, Gesichter und Kraftfahrzeugkennzeichen im Internet unkenntlich zu machen. Unkenntlich machen in diesem Sinne heißt allerdings lediglich, dass Gesichter und Kraftfahrzeugkennzeichen nicht mehr „oder nur mit unverhältnismäßig hohem Aufwand" kenntlich gemacht werden können. Alle unterzeichnenden Dienste sollen von einer gemeinsamen Plattform aus erreicht werden. Kontrolliert wird die Einhaltung des Kodex von den betrieblichen Datenschutzbeauftragten der betreffenden Unternehmen. Auch soll ein Gremium der „freiwilligen Selbstkontrolle" eingerichtet werden. Als Sanktionen für Verstöße sind Abhilfeaufforderungen, Rügen, eine Vertragsstrafe bis zu 20 000 Euro und der Ausschluss von dem Kodex vorgesehen. Die Formulierungen des Datenschutz-Kodex der Geodatenwirtschaft lassen vermuten, dass Google Street View der einzige Dienst ist und bleiben wird, der das Recht der Betroffenen auf Vorabwiderspruch anerkennt; es sei denn, es hätten sich schon vor Veröffentlichung des Kodex Geodatenfirmen verpflichtet, Vorabwidersprüche umzusetzen.

Heute sind Google Street View und ähnliche Dienste kein öffentliches Thema mehr. Ob es überhaupt noch Menschen gibt, die von ihrem Recht Gebrauch machen, auch nach der Onlinestellung des Dienstes gegen die Veröffentlichung der von ihnen bewohnten Häuser zu widersprechen, indem sie in der Sprache von Google „ein Problem melden", werden wir wahrscheinlich nie erfahren.

1.1.4 Ein Problem melden

Wer ein Problem mit dem Ausbremsen der öffentlichen Debatte hat, findet keine Internetanwendung, der sie oder er das melden kann. Ein Ort hierfür wäre wieder die Öffentlichkeit. Aber es ist schwer, das Thema noch einmal anzusprechen, nachdem der Bundesinnenminister deutlich gemacht hat, dass diejenigen, die dies tun, übertrieben empfindlich sind und über Kinkerlitzchen die wahren Probleme, die sich hinter der „roten Linie" abspielen, übersehen. Dabei entscheidet in unserer Demokratie doch das Volk, die Menschen. Sie haben sich in einer riesigen Woge des öffentlichen Interesses zu dem Thema informationelle Selbstbestimmung geäußert. Der verfassungsmäßige Umgang mit einer solchen öffentlichen Meinungsäußerung wäre die Diskussion über ein Gesetz gewesen, denn über Gesetze drückt sich in einer Demokratie aus, was der Souverän, was die Menschen wollen. Resultat war hier aber keine gesetzliche Regelung des Souveräns, sondern die Befugnis derjenigen, die von der Anwendung wirtschaftlich profitieren, den Menschen auch künftig Zugeständnisse von ihren Gnaden anzubieten. Durch zeitliches Taktieren und das Umlenken der Debatte ist die Kraft der Welle des öffentlichen Interesses gebrochen.

Dagegen hilft nur, Gesetzen, die das Persönlichkeitsrecht wirksam schützen können, die aber häufig als Verbündete des Bürokratismus verschrien sind, mehr gesellschaftliche Wertschätzung entgegenzubringen. Anders als der Bundesinnen-

minister mit seinem Rote-Linie-Gedanken meint, müssen wir uns dafür einsetzen, dass die Idee des Grundgesetzes lebt, nach der Freiheit nicht Gesetzlosigkeit ist. Der demokratische Gesetzgeber gestaltet den Raum der Freiheit der einen, die für andere Einschränkungen bedeuten kann, durch Regelungen. Der Bundesinnenminister hat sich im hier betrachteten Fall seiner Aufgabe entzogen, dem Parlament einen entsprechenden Gesetzgebungsvorschlag zu machen. Er hat stattdessen die Regelungsmacht der einen, sowieso schon mächtigeren Seite überlassen. Wenn sich die Geodatenwirtschaft, die ja nicht der öffentlichen Willensbildung verpflichtet ist, selbst reguliert, werden all die unterschiedlichen Meinungen, die sich in diesem Sommer artikuliert haben, nicht in den Entscheidungsprozess eingehen. Sie können daher die Qualität der Entscheidung nicht erhöhen.

Wir sollten uns nicht einreden lassen, dass wir uns in der öffentlichen Debatte mit Kleinigkeiten beschäftigt haben, immerhin war es unser Grundrecht auf Selbstbestimmung, und zwar auf informationelle Selbstbestimmung, das wir ausgeübt haben. Wir haben nicht alles so geschehen lassen, wie es sich diejenigen, die an den Straßenansichten verdienen, ausgedacht haben. Wir haben in die eine oder andere Richtung bewusst entschieden. Und allein das war wichtig. Und dieses Recht zu entscheiden, „Ja“ oder „Nein“ zu sagen, ist es, das wir verteidigen sollten. Am sichersten ist es, wenn es ein Gesetz ist, das uns dieses Recht verbürgt. Und wenn es keines gibt, dann sollten wir das laut als Problem melden.

1.2 Beschäftigtendatenschutz – oder: Wie es mit einem Gesetz schlimmer kommen kann als ohne

Aber nicht jedes Gesetz ist geeignet, das Grundrecht auf informationelle Selbstbestimmung wirklich vor Verletzungen zu schützen. Ein Beispiel für ein solches Gesetz, das das Grundrecht auf informationelle Selbstbestimmung sogar gefährdet, indem es weitreichende Eingriffsbefugnisse schafft, ist der Gesetzentwurf der Bundesregierung zum Beschäftigtendatenschutz.

Seit dem Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983 fordern Datenschützerinnen und Datenschützer ein eigenständiges Beschäftigtendatenschutzgesetz. Diese Forderung wurde in der Öffentlichkeit nach den Datenmissbrauchsskandalen der letzten Jahre noch viel lauter, weil sich diese in den prominentesten Fällen auf Verletzungen des Grundrechts auf informationelle Selbstbestimmung im Beschäftigungsverhältnis bezogen. Genannt seien hier stellvertretend die Videoüberwachung bei Lidl, das Beschäftigtenscreening bei der Deutschen Bahn und die Telekommunikationsüberwachung der Beschäftigten bei der Telekom und der Deutschen Bahn. Der starke öffentliche Druck führte zur Einführung eines neuen § 32 im Bundesdatenschutzgesetz. Dieser reicht allerdings nicht aus, um die vielfältigen datenschutzrechtlichen Themen im Arbeitsverhältnis zu regeln und vermag deshalb die Rechte der Beschäftigten nicht angemessen zu wahren.

Wie schon fast alle ihrer Vorgängerinnen seit dem Jahr 1983 nahm sich auch die amtierende Bundesregierung vor, spezielle gesetzliche Grundlagen für den Beschäftigtendatenschutz zu formulieren. In der Entscheidung des Koalitionsvertrages, den Beschäftigtendatenschutz nicht in einem eigenen Gesetz, sondern in einem Kapitel im Bundesdatenschutzgesetz zu regeln, lag gleichzeitig auch die Entscheidung über die Federführung innerhalb der Bundesregierung. Für das Bundesdatenschutzgesetz ist das Bundesministerium des Innern, für Gesetze im Zusammenhang mit Beschäftigungsverhältnissen ist das Bundesministerium für Arbeit und Soziales federführend. Dieser Zuständigkeitszuweisung entsprechend legte das Bundesministerium des Innern im Frühsommer des Berichtsjahrs einen Änderungsentwurf zum Bundesdatenschutzgesetz vor, mit dem dem Gesetz ein Kapitel über den Beschäftigtendatenschutz hinzugefügt werden sollte.

Nach Auffassung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder verfehlt dieser Entwurf das angestrebte Ziel eines zeitgemäßen und verbesserten Schutzes der Beschäftigten vor Überwachung und übermäßiger Kontrolle. Der Entwurf verschlechtert im Gegenteil das durch die langjährige arbeitsgerichtliche Rechtsprechung erreichte Datenschutzniveau in Beschäftigungsverhältnissen, das die Beschäftigten bislang vor übermäßiger Überwachung schützte. Auch fehlen im Entwurf Regelungen für wesentliche Fragen und Probleme, die sich in der Praxis täglich stellen. Die Konferenz der Datenschutzbeauftragten forderte deshalb im Juni insbesondere,

— die im Gesetzentwurf vorgesehene Erlaubnis zur Datenverarbeitung bei Verhaltens- und Leistungskontrollen an strenge Voraussetzungen zu knüpfen,

— die im Entwurf vorgesehene allgemeine Erlaubnis zur Verarbeitung und Nutzung von Beschäftigtendaten zur „Verhinderung und Aufdeckung von Vertragsverletzungen zulasten des Arbeitgebers, Ordnungswidrigkeiten und Straftaten" einzuschränken. Maßnahmen, die zu einer ständigen Kontrolle der Beschäftigten führen oder den Betroffenen den Eindruck einer umfassenden Überwachung am Arbeitsplatz vermitteln (wie die ständige Videoüberwachung oder regelmäßiges Aufzeichnen, Mitschneiden oder Mithören von Ferngesprächen), können wegen Verstoßes gegen das Grundrecht auf informationelle Selbstbestimmung nicht zulässig sein,

— die im Entwurf vorgesehene Befugnis von Arbeitgebern zu streichen, im Internet verfügbare Informationen generell nutzen zu dürfen, auch wenn diese durch Dritte ohne Kenntnis der Betroffenen und somit häufig rechtswidrig eingestellt wurden. Damit wird vom datenschutzrechtlichen Grundsatz der Direkterhebung beim Betroffenen abgewichen und Arbeitgeber werden geradezu eingeladen, im Internet und in sozialen Netzwerken systematisch nach dort vorhandenen Informationen über Bewerber und Beschäftigte zu recherchieren,

— die Möglichkeiten der Einsichtnahme in die elektronische Kommunikation von Beschäftigten durch Arbeitgeber strikt zu begrenzen,

— keine „Einwilligungen" von Beschäftigten in Datenschutzverletzungen zu erlauben, weil Einwilligungen im Arbeitsverhältnis in den meisten Fällen mangels Freiwilligkeit nicht rechtswirksam erteilt werden können.

In seiner Stellungnahme zum Gesetzentwurf beschloss der Bundesrat im November 2010 eine Vielzahl von Änderungsanträgen, die bis auf wenige Ausnahmen das Datenschutzniveau des Gesetzentwurfs deutlich erhöhen und dem durch die arbeitsgerichtliche Rechtsprechung erreichten Niveau annähern würden und viele Kritikpunkte der Konferenz der Datenschutzbeauftragten teilen.

Im Zusammenhang mit der Begründung des Arbeitsverhältnisses fordert der Bundesrat beispielsweise eine ausdrückliche Regelung, wonach der Arbeitgeber nur dann Auskunft über eine Schwangerschaft einer Beschäftigten verlangen darf, wenn die gesamte Dauer eines befristeten Arbeitsverhältnisses in die gesetzliche Mutterschutzfrist fallen würde.

Die automatisierte Auswertung von vorhandenen und für andere Zwecke erhobenen Daten der Beschäftigten wird „Screening" genannt. Wie die Konferenz der Datenschutzbeauftragten fordert der Bundesrat, dass Voraussetzung eines solchen Screenings das Vorliegen von tatsächlichen Anhaltspunkten für das Vorliegen einer Straftat sein muss. Es müsse daneben gesetzlich klargestellt werden, dass die Durchführung eines Screenings geeignet und erforderlich sein muss, um die Aufdeckung der Tat zu erreichen, und dass der verfolgte Zweck in einem angemessenen Verhältnis zu dem durchgeführten Verfahren stehen muss. Auch schwerwiegende Pflichtverletzungen vermöchten die Durchführung einer solchen – den Datenschutz in besonderer Weise gefährdenden – Maßnahme nicht zu rechtfertigen. Nur mithilfe dieser Vorgaben könne sichergestellt werden, dass etwa ein Diebstahl geringwertiger Sachen, der von der aktuellen Rechtsprechung teilweise als schwerwiegende Pflichtverletzung angesehen werde, kein Datenscreening rechtfertigen könne. Auch dürften nur die den – durch das Screening ermittelten – konkreten Verdachtsfall betreffenden Daten personalisiert werden.

Die im Entwurf vorgesehene Befugnis zur verdeckten Datenerhebung zur Verhinderung von im Zusammenhang stehenden weiteren Straftaten oder schwerwiegenden Pflichtverletzungen des Beschäftigten lehnt auch der Bundesrat ab. Eine verdeckte Datenerhebung allein aus präventiven Gründen sei wegen der dem Arbeitgeber zur Verfügung stehenden arbeitsrechtlichen Möglichkeiten nicht erforderlich. Auch müsse anders, als das im Entwurf der Fall sei, gewährleistet sein, dass die verdeckte Erhebung selbst beim Verdacht einer schwerwiegenden Pflichtverletzung als gravierender Eingriff in das Persönlichkeitsrecht des Betroffenen nur als äußerstes Mittel eingesetzt wird, wenn eine offene Ermittlung deutlich erschwert sei beziehungsweise erheblich geringere Erfolgsaussichten habe.

Sehr zur Freude der Konferenz der Datenschutzbeauftragten des Bundes und der Länder setzt sich der Bundesrat für die Streichung einer Vorschrift ein, nach der sich ein Beschäftigter erst dann an die Datenschutzaufsicht, also in der Regel die Landesbeauftragten für den Datenschutz, wenden dürfen soll, wenn der Arbeitgeber einer entsprechenden Beschwerde des Beschäftigten nicht abgeholfen hat. Nach

dem Entwurf sollen sich die Beschäftigten also im Konfliktfall zunächst an die Arbeitgeber wenden müssen, denen sie ja eine Verletzung ihrer Rechte gerade vorwerfen. Die Praxis zeigt, dass die Beschäftigten aus Sorge um Nachteile im Rahmen der weiteren Beschäftigung häufig sogar anonym bleiben wollen (vergleiche Ziffer 12.4 dieses Berichts). Deshalb weist der Bundesrat auch darauf hin, dass die vorgesehene Regelung der Europäischen Union-Datenschutzrichtlinie widerspricht, die jeder Person das einschränkungslose Recht gewährt, sich zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an die zuständige Kontrollstelle zu wenden.

Mitte Dezember 2010 legte die Bundesregierung ihre Gegenäußerung zur Stellungnahme des Bundesrats vor. Einzige Verbesserung darin aus datenschutzrechtlicher Sicht ist die Rücknahme des Regelungsvorschlags, nach dem die Beschäftigten sich bei Beschwerden über Datenschutzverstöße zunächst an den Arbeitgeber selbst wenden müssen, bevor sie die datenschutzrechtlichen Aufsichtsbehörden kontaktieren. Alle anderen datenschutzfreundlichen Änderungsanträge des Bundesrats wurden von der Bundesregierung mit der Formulierung zurückgewiesen, die Bundesregierung teile die Auffassung des Bundesrats nicht.

Jetzt bleibt zu hoffen, dass zumindest der Bundestag die nicht nur von der Datenschutzkonferenz geäußerte Kritik und die Änderungsanträge des Bundesrats aufnimmt. Allerdings steht nach der Änderung des Bundesdatenschutzgesetzes unter nur geringer Beachtung der Änderungsanträge des Bundesrats im Jahr 2009 und nach dem eben beschriebenen Abschmettern des Bundesratsgesetzes zu Geodatendiensten im Berichtsjahr datenschutzrechtlich gesehen zu erwarten, dass die parteiübergreifenden Initiativen und Änderungsanträge des Bundesrats von Bundesregierung und Bundestag ignoriert werden. Dabei handelt es sich bei dem Bundesrat doch um ein Gremium, das den politischen Willensbildungsprozess in diesem Land zumindest dann gut abbildet, wenn seine Entscheidungen wie in allen genannten Fällen von der deutlichen Mehrheit der Bundesländer, unabhängig von der politischen Zusammensetzung ihrer Regierungen, getragen werden. Übrigens ist der Bundesrat auch ein Gremium, in dem Lobbyarbeit deutlich mühseliger ist als im Bundestag.

Damit das Grundrecht der informationellen Selbstbestimmung der Beschäftigten nicht hinter den bereits erreichten Stand zurückfällt, wäre es sehr wichtig, die datenschutzfreundlichen Änderungsvorschläge des Bundesrats jedenfalls dieses Mal zu berücksichtigen.

1.3 Vorratsdatenspeicherung – oder: Es auch nach herben Niederlagen einfach noch mal probieren, als wäre nichts geschehen

Ein weiteres Beispiel dafür, dass Gesetze das Grundrecht auf informationelle Selbstbestimmung nicht in jedem Fall schützen, ist der Bereich der Vorratsdatenspeicherung unserer Telekommunikationsverbindungsdaten (wer telefoniert oder mailt mit wem, zu welcher Zeit und wie lange – und bei Mobiltelefonen zusätzlich: von welchem Ort aus?). Die öffentliche Debatte zu diesem Thema nahm im Berichtsjahr einen bemerkenswerten Verlauf:

Am 2. März 2010 entschied das Bundesverfassungsgericht, dass das Gesetz zur Neuregelung der Telekommunikationsüberwachung, das eine vorsorgliche anlasslose sechsmonatige Speicherung der Telekommunikationsverbindungsdaten aller Menschen angeordnet hatte, verfassungswidrig ist. Die Karlsruher Richterinnen und Richter machten deutlich, dass es sich bei einer solchen Speicherung um einen besonders schweren Eingriff mit einer Streubreite handelt, wie sie die Rechtsordnung bisher nicht kennt. Auch Verkehrsdaten würden inhaltliche Rückschlüsse bis in die Intimsphäre ermöglichen und damit aussagekräftige Persönlichkeits- oder Bewegungsprofile liefern. Weil keine ausreichende Datensicherheit gewährleistet sei und die Datenverwendung von den Bürgern nicht bemerkt werde, sei die Vorratsdatenspeicherung in ihrer bisherigen Form geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen könne. Das Bundesverfassungsgericht ordnete deshalb in seiner Entscheidung an, dass alle seit Erlass des Gesetzes erhobenen Daten unverzüglich zu löschen seien.

Nach Auffassung des Gerichts soll eine Vorratsdatenspeicherung unter einer Reihe enger Vorgaben allerdings möglich sein. Hierzu sollen unter anderem die Gewährleistung eines besonders hohen Standards der Datensicherheit und das Vor-

liegen von schwerwiegenden Straftaten gehören. Das Bundesverfassungsgericht formulierte also sehr hohe Hürden für ein Gesetz zur Telekommunikationsüberwachung. Aus Sicht des Grundrechts auf informationelle Selbstbestimmung wäre es konsequent gewesen, wenn das Bundesverfassungsgericht noch weiter gegangen wäre und eine anlasslose Massenspeicherung von Verkehrsdaten für grundsätzlich nicht mit dem deutschen Verfassungsrecht vereinbar erklärt hätte. Dies hätte auch damit begründet werden können, dass auch die Europäische Union (EU), insbesondere die Justizkommissarin Viviane Reding, schon zuvor Zweifel an der Übereinstimmung der Vorratsdatenspeicherung mit der EU-Grundrechtecharta artikuliert hatte. In der sich anschließenden öffentlichen Debatte dominierten diejenigen, die eine anlasslose Massenspeicherung von Verbindungsdaten auf Vorrat grundsätzlich ablehnten.

Die Bundesjustizministerin hatte gleich nach dem Urteil angekündigt, die verbliebenen Spielräume für ein Gesetz zu dieser Thematik zu prüfen und dabei auch die Ergebnisse der europäischen Prüfungen zu beachten. Die Bremische Bürgerschaft hat noch im November 2010 Zweifel an der Übereinstimmung der Vorratsdatenspeicherung mit EU-Recht artikuliert und den Senat aufgefordert, im Bundesrat darauf hinzuwirken, dass sich die Bundesregierung auf EU-Ebene entschieden gegen die Vorratsdatenspeicherung einsetzt. Anfang des Jahres 2011 hat die Bundesjustizministerin ein Eckpunktepapier vorgelegt, in dem sie äußert, es sei absehbar, dass es zu Änderungen der EU-Richtlinie kommen werde, deren Umfang und Tragweite gegenwärtig niemand verlässlich vorhersagen könne. Die Bundesjustizministerin schlägt daher vor, jetzt gesetzliche Voraussetzungen dafür zu schaffen, die bei den Telekommunikationsunternehmen aus geschäftlichen Gründen bereits vorhandenen Verkehrsdaten anlassbezogen zu sichern („einzufrieren"). Sie sollten den Strafverfolgungsbehörden unter Richtervorbehalt eine begrenzte Zeit zur Verfügung stehen, um schwere Straftaten verfolgen zu können. Im Internetbereich solle eine eng befristete Speicherung von Verkehrsdaten zu dem Zweck erfolgen dürfen, Bestandsdatenauskünfte, also eine Zuordnung dynamischer IP-Adressen (Adressen in Computernetze) zu Personen, zu ermöglichen.

Doch wird eine solche Regelung den Befürwortern der Vorratsdatenspeicherung ausreichen? Der Bundesinnenminister geht davon aus, ohne eine „Mindestspeicherfrist für Verkehrsdaten", also ohne Vorratsdatenspeicherung der Verbindungsdaten, komme die Strafverfolgung zum Erliegen. Auch seine Ministerkollegen aus den Ländern schlossen sich in einer Entschließung der Innenministerkonferenz im Oktober des Berichtsjahrs dieser Auffassung an. Gegenwärtig bestehe eine erhebliche Schutzlücke in der Kriminalitätsbekämpfung. Die Strategie der Befürworter der Vorratsdatenspeicherung von Verbindungsdaten bleibt eine Nadelstichtaktik. Gebetsmühlenartig wird wiederholt, dass seit dem Urteil des Bundesverfassungsgerichts eine effektive Strafverfolgung im Internet kaum mehr möglich sei. Die Beweise hierfür bleiben die Befürworter der Vorratsdatenspeicherung schuldig. Noch in einer Bundestagsdrucksache vom Ende November des Berichtsjahrs antwortete die Bundesregierung, es werde „weiterhin geprüft", welche Delikte bei einem vollständigen Verzicht auf die Nutzung der Vorratsdaten durch die Sicherheitsbehörden nicht mehr verfolgt werden könnten. Auch daher spricht viel für die Vermutung meines bayerischen Kollegen Dr. Thomas Petri, dass die Speicherung von anderen Telekommunikationsdaten als den von der Bundesjustizministerin erwähnten Daten zur Zuordnung dynamischer IP-Adressen zu Personen, also etwa die Speicherung von Standortdaten und Angaben zur Verbindungsdauer, in der Praxis nur eine untergeordnete Rolle spielt.

Im Verlauf des Jahres 2011 werden wir beobachten können, ob es den Befürworterinnen und Befürwortern der Vorratsdatenspeicherung gleichwohl gelingt, die Öffentlichkeit, die sich so deutlich gegen die Vorratsdatenspeicherung gewendet hatte, davon zu überzeugen, dass die Telekommunikationsdaten aller Menschen auf Vorrat gespeichert werden müssen.

1.4 Modernisierung des Datenschutzrechts

Mein Bericht über die Google Street-View-Debatte des letzten Jahres (vergleiche Ziffer 1.1 dieses Berichts) ist zu einem Plädoyer für das Gesetz als einzigem wirksamen Werkzeug zum Schutz des Grundrechts auf informationelle Selbstbestimmung gegen Verletzungen durch Handlungen, die sich auf Wirtschaftsfreiheiten berufen, geworden. Er zeigt, dass die Stoßrichtung der Debatte über Bürokratie-

abbau falsch ist, wenn sie Gesetze unter den Generalverdacht stellt, unnötige Bürokratie zu schaffen. Dieser Verdacht ist unbegründet und – sofern es ihm wie im Fall der Regelungen über Widerspruchsrechte gegen Straßenansichten gelingt, die Verabschiedung von Gesetzen zu verhindern – sogar gefährlich. Nur Gesetze können verbindlich die Regeln formulieren, die die Freiheit der einen von der Freiheit der anderen abgrenzen. Die Beispiele Beschäftigtendatenschutz und Vorratsdatenspeicherung zeigen allerdings, dass es zum wirksamen Schutz des Grundrechts auf informationelle Selbstbestimmung nicht ausreicht, irgendein Gesetz zu verabschieden. Es müssen gesetzliche Formulierungen gefunden werden, denen es gelingt, verbindliche Grenzen zu formulieren, die das Grundrecht auf informationelle Selbstbestimmung, beispielsweise im Fall der Nutzung fremder personenbezogener Daten zu Zwecken des eigenen ökonomischen Gewinns, auch vor Handlungen zu schützen, die grundsätzlich von der Berufsfreiheit und dem Recht auf Eigentum geschützt sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat viele Bereiche gefunden, in denen es an gesetzlichen Regelungen mangelt oder es bestehenden Regelungen nicht gelingt, das Grundrecht auf informationelle Selbstbestimmung als Funktionsbedingung einer menschenwürdigen Informationsgesellschaft wirksam zu schützen. Das im Berichtsjahr vorgelegte Eckpunktepapier „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ der Konferenz reagiert darauf, dass wir uns im Zeitalter der allgegenwärtigen, oftmals unbemerkten Datenverarbeitung befinden. Beispielhaft seien hier neben Videokameras nur RFID-Chips (Funkchips), Navigationsgeräte, elektronische Sensoren, die Raumtemperaturen regeln, und Messeinrichtungen in Kraftfahrzeugen genannt. In dieser Situation brauchen wir gesetzliche Regelungen, die technikneutral sind. Sie müssen für die Datenschutzgrundsätze Erforderlichkeit, Zweckbindung, Transparenz, Datenvermeidung und Datensparsamkeit verbindliche Mindeststandards festlegen. Als neu formuliertes Prinzip muss das grundsätzliche Verbot der Profilbildung normiert werden. Die Rechte der Betroffenen müssen gestärkt und Lücken im datenschutzrechtlichen Sanktionssystem geschlossen werden. Im Bereich des Internet muss eine unbeobachtete Kommunikation und Nutzung gewährleistet werden. Die Rechte der Betroffenen im Netz müssen durch besondere Schutzmechanismen gewährleistet werden und durchsetzbar sein. Wegen der Internationalität des Internet müssen neben nationalen Regelungen internationale Vereinbarungen getroffen werden.

Diese Eckpunkte haben wir zur Diskussion gestellt, um der öffentlichen Debatte überzeugende Argumente für neue und/oder konkretisierte gesetzliche Regelungen zum Schutz der Grundrechte auf informationelle Selbstbestimmung und auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu liefern. Wir hoffen und werden darum kämpfen, dass diese Argumente Gehör finden.

1.5 Medienkompetenz: Der Verzicht auf den erhobenen Zeigefinger

Medienkompetenz für Kinder und Jugendliche ist in aller Munde. In Bremen hat sich im Berichtsjahr der runde Tisch Bremische Medien Kompetenz, kurz BreMeKo, konstituiert. Er versammelt über 30 Organisationen, die an der Schaffung und Stärkung von Medienkompetenz in Bremen arbeiten. Bei der Vorstellung der Organisationen zeigte sich eine wichtige Gemeinsamkeit. Bremische Medienkompetenzvermittlerinnen und Medienkompetenzvermittler verzichten gern auf den erhobenen Zeigefinger.

Auch wird in Bremen der Begriff Medienkompetenz sehr weit ausgelegt. Medienkompetenz beinhaltet danach zwar auch, aber eben nicht nur, die Technik zu beherrschen, also beispielsweise im Bereich des Datenschutzes technisch vorgesehene Schutzmöglichkeiten korrekt bedienen zu können. Wichtig ist es, im Internet aber genauso wie bei der Lektüre von Tageszeitungen oder Wahlprogrammen auch, einordnen zu lernen, wer was wann weshalb schreibt und von mir wissen will. Medienkompetenz in diesem weiten Sinne beinhaltet auch die Kritikfähigkeit gegenüber dem Gelesenen, also die Fähigkeit zu erkennen, dass Namen Schall und Rauch sind, dass Meinungen interessengeleitet und auf Verhaltenssteuerung zum eigenen Nutzen angelegt sind, dass Freundinnen und Freunde in der Onlinewelt etwas anderes sind als im echten Leben. Die demokratische Nutzung von Informationen setzt diese Medienkompetenz im Sinne der Fähigkeit zur Kritik voraus. Auf der Internetseite www.klicksafe.de finden Kinder, Jugendliche und ihre Eltern

viele Informationen und Anregungen in diese Richtung. In Bremen informiert das ServiceBureau Jugendinformation unter www.servicebureau.de.

In einer überregionalen Tageszeitung fand sich kürzlich ein Artikel über Cybermobbing (Belästigung, Bedrängung und Nötigung anderer Menschen mit Hilfe elektronischer Kommunikationsmittel über das Internet). Genauer ging es um eine Internetseite, auf der Schülerinnen und Schüler aufgefordert werden, anonym ihre Mitschülerinnen und Mitschüler zu beleidigen. Direkt daneben stand die Nachricht über das Verfahren gegen einen Psychologen, der – mutmaßlich im Auftrag von führenden Kräften eines Finanzministeriums – Steuerfahnderinnen und Steuerfahndern, die unliebsame Untersuchungen angestrengt hatten, fälschlich attestierte, sie seien psychisch krank. Wenn sogar staatliche Stellen in Verdacht geraten, zu mobben, um unliebsame Beamtinnen und Beamte aus dem Dienst zu entfernen, wie sollen Kinder und Jugendliche da begreifen, dass die Rechte anderer Grenze ihrer Freiheit sind, dass die Würde des Menschen unantastbar ist? Da haben Staat und Erwachsene noch viel positiv vorzuleben. Und aus einer vermeintlich überlegenen Position erhobene Zeigefinger sind nicht am Platz, da haben die bremischen Medienkompetenzvermittlerinnen und Medienkompetenzvermittler recht.

Dass die Nutzerinnen und Nutzer des Internet sich andererseits der Gefahren für ihr Grundrecht auf informationelle Selbstbestimmung bewusster sind, als viele denken, und dabei ihren Humor behalten, zeigt der Tweet (ein Beitrag im Web unter Twitter). Wie formulierte das Bundesverfassungsgericht doch so schön? „Das diffuse Gefühl des Beobachtetseins“ durch Staat und andere interessierte Kreise – es bleibt uns auch im Jahr 2011 erhalten.

Dr. Imke Sommer

Die Landesbeauftragte für Datenschutz und
Informationsfreiheit der Freien Hansestadt Bremen

2. Bremische Bürgerschaft – Ergebnisse der Beratungen des 32. Jahresberichts

Bericht und Antrag des Ausschusses für Informations- und Kommunikationstechnologie und Medienangelegenheiten zum 32. Jahresbericht der Landesbeauftragten für Datenschutz vom 26. März 2010 (Drucksache 17/1240) und zur Stellungnahme des Senats vom 24. August 2010 (Drucksache 17/1407)

I. Bericht

Die Bürgerschaft (Landtag) überwies in ihrer Sitzung am 21. April 2010 den 32. Jahresbericht der Landesbeauftragten für den Datenschutz vom 26. März 2010 (Drucksache 17/1240) und in ihrer Sitzung am 29. September 2010 die dazu erfolgte Stellungnahme des Senats vom 24. August 2010 (Drucksache 17/1407) an den Ausschuss für Informations- und Kommunikationstechnologie und Medienangelegenheiten zur Beratung und Berichterstattung.

Der Ausschuss beschäftigte sich in seiner Sitzung am 29. Oktober 2010 mit dem 32. Jahresbericht sowie der Stellungsnahme des Senats und stellte bei den nachfolgend aufgeführten Punkten Beratungsbedarf fest:

1. Ziffer 5.1 Künstliche DNA
2. Ziffer 5.2 Stopp der Jugendgewalt
3. Ziffer 5.8 Datenschutzkonzepte beim Stadtamt Bremen
4. Ziffer 7.3 BAgIS/ARGE Job-Center-Bremerhaven
5. Ziffer 7.10 Auslagerung der Abrechnungsprüfung durch die Kassenärztliche Vereinigung Bremen (KVHB)

In seiner Sitzung am 29. Oktober 2010 erörterte der Ausschuss die beratungsbedürftigen Punkte mit der Landesbeauftragten für den Datenschutz unter Hinzuziehung von Vertreterinnen und Vertretern der betroffenen Ressorts.

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

1. Künstliche DNA (Ziffer 5.1):

Der Ausschuss hat zur Kenntnis genommen, dass die Landesbeauftragte für Datenschutz erhebliche datenschutzrechtliche Bedenken gegen den Einsatz von DNA-Sprühanlagen durch Private hat. Das Markieren von Personen mittels künstlicher DNA stelle aus ihrer Sicht einen Grundrechtseingriff dar, für den als Maßnahme der Strafverfolgung durch Private keine gesetzliche Rechtfertigung existiere. Diese rechtlichen Bedenken gegen den Einsatz von DNA-Sprühanlagen werden vom Senator für Inneres und Sport nicht geteilt. Um zumindest einen verantwortungsvollen Umgang der Betreiber mit den DNA-Sprühanlagen zu gewährleisten, haben sich die Landesbeauftragte und der Senator für Inneres und Sport darauf verständigt, dass die Polizei künftig von den Betreibern die Einhaltung bestimmter Verpflichtungen einfordert. So sind unter anderem die Mitarbeiterinnen und Mitarbeiter im Umgang mit den Anlagen zu schulen sowie deutlich sichtbare Hinweisschilder an den jeweiligen Gebäuden anzubringen. Der Ausschuss begrüßt, dass die Polizei in diesem Bereich durch die Kontrolle der Betreiber von DNA-Sprühanlagen eine größere Verantwortung übernimmt. Nun müsse abgewartet werden, wie sich dieses Verfahren in der Praxis bewähre.

2. Stopp der Jugendgewalt (Ziffer 5.2):

Der Ausschuss hat zur Kenntnis genommen, dass es aufgrund fehlender Rechtsgrundlagen aus datenschutzrechtlicher Sicht höchst problematisch ist, im Rahmen von behördenübergreifenden Fallkonferenzen Informationen über eine Person auszutauschen. Um diese rechtlichen Hürden zu überwinden, haben sich die Landesbeauftragte und die beteiligten senatorischen Dienststellen darauf verständigt, die Übermittlung der Informationen auf eine Einwilligung der Betroffenen zu stützen und entsprechend eine Einwilligungserklärung auszuarbeiten. Da die Erteilung der Einwilligung durch die Betroffenen auf freiwilliger Basis erfolgt und diese umfassend über die Bedeutung der Einwilligung aufgeklärt werden, hält der Ausschuss den gefundenen Weg für eine gute Lösung.

3. Datenschutzkonzepte beim Stadtamt Bremen (Ziffer 5.8):

Der Ausschuss hat sich berichten lassen, dass das bislang fehlende und von der Datenschutzbeauftragten immer wieder geforderte Rahmendatenschutzkonzept

beim Stadtamt Bremen nunmehr vorliege, ebenso wie das IT-Betriebskonzept. Ferner sei bereits damit begonnen worden, diese Konzepte in den Fachbereichen umzusetzen. Aufgrund von personellen Verstärkungen des Stadtamts in einzelnen Fachbereichen erhofft sich der Ausschuss, dass das Rahmenkonzept möglichst zeitnah mit Inhalten gefüllt wird und datenschutzrechtliche Erfordernisse künftig schneller umgesetzt werden können.

4. BAgIS/Arbeitsgemeinschaft (ARGE) Job-Center-Bremerhaven (Ziffer 7.3):

Der Ausschuss hat zur Kenntnis genommen, dass es im Berichtsjahr zahlreiche Beschwerden über die mangelnde Vertraulichkeit von Gesprächen zwischen Kundin beziehungsweise Kunde und Mitarbeiter der Bremer Arbeitsgemeinschaft für Integration und Soziales (BAgIS) gegeben habe. Teilweise würden mehrere Gespräche in einem Raum geführt oder es sei Sicherheitspersonal anwesend, sodass unbefugte Dritte diese sensiblen Gespräche mithören könnten. Die Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales sowie die BAgIS selbst sind sich dieses Problems bewusst und haben im Rahmen der räumlichen Möglichkeiten versucht, durch zusätzliche Sichtschutzwände ein größeres Maß an Vertraulichkeit der Gespräche zu schaffen. Sie haben gegenüber dem Ausschuss jedoch auch deutlich gemacht, dass das Grundproblem aufgrund der eingeschränkten Raummöglichkeiten nicht zu lösen sei, da die Raumkonzepte Einzelbüros für die Mitarbeiterinnen und Mitarbeiter nicht vorsähen und auch nicht zuließen. Eine Verbesserung der Einhaltung von datenschutzrechtlichen Bestimmungen sei aber bereits durch entsprechende Schulungen der Mitarbeiterinnen und Mitarbeiter sowie Entfristungen zahlreicher Verträge erreicht worden. Ferner bestehe auch für das eingesetzte Sicherheitspersonal die Verpflichtung zur Einhaltung von datenschutzrechtlichen Bestimmungen.

5. Auslagerung der Abrechnungsprüfung durch die Kassenärztliche Vereinigung Bremen (Ziffer 7.10):

Die Kassenärztliche Vereinigung Bremen (KVHB) hatte die Kassenärztliche Vereinigung Bayerns (KVB) damit beauftragt, für sie Daten der vertragsärztlichen Leistungsabrechnung einer Plausibilitätsprüfung und einer Prüfung der rechnerischen und sachlichen Richtigkeit zu unterziehen. Nach Auffassung der Landesbeauftragten für Datenschutz gibt es für diese Weitergabe von Sozialdaten keine einschlägige Rechtsgrundlage. Die KVHB sowie die Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales teilen diese Rechtsauffassung nicht, sondern halten das Vorgehen für rechtlich zulässig. Dennoch hat sich die KVHB bereit erklärt, die Übermittlung der Daten an die KV Bayern zunächst einzustellen, da die Angelegenheit aufgrund der grundsätzlichen Bedeutung auch dem Bundesministerium für Gesundheit zur Stellungnahme vorläge. Der Ausschuss ist der Auffassung, dass zunächst abgewartet werden sollte, wie sich das Bundesgesundheitsministerium in dieser Sache äußere. Zu gegebener Zeit werde sich der Ausschuss dann erneut mit diesem Fall beschäftigen. Es wird insbesondere zu prüfen sein, ob sich die getroffenen Aussagen zu dieser Fallkonstellation auf die Fälle der hausarztzentrierten Verträge anwenden lassen.

II. Antrag

Die Bürgerschaft (Landtag) möge beschließen:

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

3. Behördliche und betriebliche Beauftragte für den Datenschutz

3.1 Workshops der behördlichen Datenschutzbeauftragten

Die Workshops mit den behördlichen Datenschutzbeauftragten der bremischen Verwaltung wurden im Berichtsjahr weiter fortgesetzt. In Bremen fand ein Workshop statt, der sich schwerpunktmäßig mit dem Thema „Verfahrensbeschreibung und Datenschutzkonzept – wie müssen sie gestaltet sein?“ befasste. Die Verfahrensbeschreibung und das Datenschutzkonzept sind wichtige Module des in den Dienststellen erforderlichen Datenschutz-Managements und für die Datenschutzbeauftragten wichtige Instrumente zur Wahrnehmung ihrer Funktion. Während die Verfahrensbeschreibung in erster Linie eine Übersicht über das jeweilige Verfahren bietet, enthält das Datenschutzkonzept konkrete Regelungen, insbesondere zum Geräteeinsatz, zu den Pflichten des Personals sowie zu Maßnahmen zur Sicher-

stellung des Datenschutzes, darunter die technischen und organisatorischen Sicherungsmaßnahmen. Im Workshop wurden insbesondere die Inhalte der Verfahrensbeschreibung, die Bedeutung der technischen und organisatorischen Maßnahmen sowie die Gestaltung von Rahmen- und Fachdatenschutzkonzepten als Untergliederung von Datenschutzkonzepten näher erläutert. Nach einem Fachreferat zum Thema hatten die Teilnehmenden ausführlich Gelegenheit, Fragen zu stellen, wovon rege Gebrauch gemacht wurde. Wegen des starken Interesses bei den Datenschutzbeauftragten wurden zu dem Thema zwei inhaltlich gleiche Veranstaltungen durchgeführt, sodass sich die Teilnehmerinnen und Teilnehmer des Workshops in zwei etwa gleich große Gruppen aufteilten. Besonderer Dank gilt der Feuerwehr Bremen, die uns freundlicherweise den Veranstaltungsraum zur Verfügung stellte.

Erneut wurde ein Workshop auch mit den behördlichen Datenschutzbeauftragten der Stadtverwaltung Bremerhaven durchgeführt. Schwerpunkt dieser Veranstaltung war das Thema „Datenschutzfragen im Zusammenhang mit Videoüberwachung". Im öffentlichen Bereich werden nunmehr schon seit vielen Jahren Videokameras für die Beobachtung und Überwachung genutzt. Die Überwachung ist nur zulässig, wenn sie unter Beachtung der einzuhaltenden datenschutzrechtlichen Anforderungen erfolgt. Im Hinblick auf die Videoüberwachung ergeben sich zahlreiche datenschutzrechtliche Fragen, an deren Lösung die Datenschutzbeauftragten in ihren Dienststellen maßgeblich beteiligt sind. Des Weiteren wurden in dem Workshop Fragen erörtert, die die Regelungen des Gesetzes über das Verfahren des elektronischen Entgeltnachweises (ELENA), insbesondere die Verhältnismäßigkeit der nach dem Gesetz vorgeschriebenen Übermittlung von Beschäftigtendaten an die bei der Deutschen Rentenversicherung Bund eingerichtete zentrale Speicherstelle, betreffen. Auch der Workshop in Bremerhaven stieß bei den behördlichen Datenschutzbeauftragten auf eine gute Resonanz.

In allen Workshops bestand darüber hinaus für die Teilnehmenden die Möglichkeit, sich über die bei ihrer Tätigkeit gesammelten Erfahrungen auszutauschen.

3.2 Amtsniederlegungen bei behördlichen Datenschutzbeauftragten

Gleich zweimal waren wir im Berichtsjahr mit Fällen befasst, in denen die behördlichen Datenschutzbeauftragten keine Möglichkeit mehr sahen, ihr Amt so wahrzunehmen, wie es notwendig gewesen wäre, und es deshalb niederlegten. Die uns aufgrund ihres besonderen Interesses am Datenschutz und hervorzuhebenden Engagements hinsichtlich der Umsetzung der datenschutzrechtlichen Anforderungen in ihren Dienststellen bekannten Datenschutzbeauftragten begründeten die Amtsniederlegungen insbesondere damit, dass sie die notwendige Unterstützung, zu der ihre Behörde nach dem Bremischen Datenschutzgesetz (BremDSG) verpflichtet ist, nicht erhalten hätten.

So führte der bisherige behördliche Datenschutzbeauftragte einer großen bremischen Behörde gleich mehrere Vorgänge an, bei denen seine rechtzeitige Beteiligung, wie sie im BremDSG vorgeschrieben ist, nicht erfolgte. Über in seiner Dienststelle neu eingesetzte Verfahren oder auch Verfahrensänderungen hätte er nach deren Inbetriebnahme erst aus der Tageszeitung oder dem Internet erfahren.

Wir wiesen die betreffende Behörde darauf hin, dass behördliche Datenschutzbeauftragte die Aufgabe haben, auf die Einhaltung der zu beachtenden Datenschutzbestimmungen hinzuwirken und diese Aufgabe in erster Linie der Prävention möglicher Verstöße gegen die Anforderungen des Datenschutzes dient. Datenschutzbeauftragte müssen daher frühzeitig über Vorhaben der automatisierten Verarbeitung personenbezogener Daten unterrichtet werden. Die für die Datenverarbeitung verantwortlichen Stellen sind verpflichtet, ihre Datenschutzbeauftragten immer dann zu konsultieren und zu unterrichten, wenn Entscheidungen bevorstehen, die sich auf die Verarbeitung personenbezogener Daten auswirken. Insbesondere, um Verarbeitungen zu vermeiden, die den datenschutzrechtlichen Anforderungen zuwiderlaufen, ist es erforderlich, keine Entscheidung ohne Kenntnis und Mitwirkung der behördlichen Datenschutzbeauftragten zu treffen.

Wir kritisierten ausdrücklich das Verhalten der Behörde und forderten sie auf, die künftige behördliche Datenschutzbeauftragte beziehungsweise den künftigen behördlichen Datenschutzbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen und insbesondere rechtzeitig an Vorhaben der Verarbeitung personenbezogener Daten zu beteiligen.

In einem anderen Fall erläuterte die bisherige Amtsinhaberin die Amtsniederlegung damit, dass es ihr nicht möglich sei, die Funktion der behördlichen Datenschutzbeauftragten fortzuführen, da die anderen von ihr dienstlich zu erfüllenden Aufgaben dies nicht zuließen und sie die für die Ausübung ihres Amtes als behördliche Datenschutzbeauftragte benötigte Unterstützung von ihrer Dienststelle nicht erhalte.

Hierzu wiesen wir die betreffende Behörde auf die gesetzliche Verpflichtung hin, der behördlichen oder dem behördlichen Datenschutzbeauftragten die für die Wahrnehmung ihrer oder seiner Aufgaben benötigte Zeit zur Verfügung zu stellen. Dabei entscheiden die behördlichen Datenschutzbeauftragten aufgrund der gesetzlich verankerten Weisungsfreiheit selbst, wie sie ihre Aufgaben erfüllen. Eine Begrenzung der zur Verfügung stehenden Zeit gefährdet die Aufgabenwahrnehmung und läuft der Weisungsfreiheit der Datenschutzbeauftragten entgegen. Machen die behördlichen Datenschutzbeauftragten darauf aufmerksam, dass die ihnen zur Verfügung gestellte Zeit zur Aufgabenerfüllung nicht ausreicht, müssen die Dienststellen dem Bedarf an zusätzlich benötigter Arbeitszeit entsprechen. Außerdem ist es den Datenschutzbeauftragten zu ermöglichen, sich angemessen und kontinuierlich fortzubilden. Nur so erhalten die Datenschutzbeauftragten die Möglichkeit, auf die Einhaltung der datenschutzrechtlichen Anforderungen, wie vom Gesetzgeber gewollt, hinzuwirken. Der Fortbildung dient auch der Kenntnisnahme von für die Aufgabenerfüllung erforderlicher Fachliteratur. Die Kosten dieser Literatur, insbesondere der benötigten Fachzeitschriften, sind von der Behörde, nicht aber von den Datenschutzbeauftragten selbst zu tragen. Auch in diesem Fall kritisierten wir ausdrücklich das Verhalten der Behörde und forderten sie auf, künftig anders zu verfahren.

Nur wenn der oder dem behördlichen Datenschutzbeauftragten die ihr oder ihm gesetzlich eingeräumten Rechte zuteilwerden, kann sie oder er den Aufgaben, wie gesetzlich vorgeschrieben, nachkommen. Dies gilt insbesondere im Hinblick auf die für die Aufgabenerfüllung benötigte Unterstützung durch die Dienststelle. Anderenfalls käme es zu einer Pro-forma-Bestellung, die der speziellen Bedeutung der Funktion bei immer umfangreicherer und vielfältiger werdenden Datenverarbeitungen in den Behörden eindeutig zuwiderliefe. Alle nach dem BremDSG zur Bestellung verpflichteten Stellen sind aufgefordert, dem Gesetz gerade in dieser Hinsicht Rechnung zu tragen.

3.3 Mindestanforderungen an betriebliche Datenschutzbeauftragte

Oftmals werden wir von Firmen oder potenziellen betrieblichen Datenschutzbeauftragten nach den Anforderungen an betriebliche Datenschutzbeauftragte hinsichtlich der Fachkunde und Unabhängigkeit gefragt. Eine pauschale Aussage hierzu zu treffen, ist nicht möglich. Dennoch möchten wir derartige Anfragen nicht unbeantwortet lassen und den Betroffenen eine Hilfe an die Hand geben. Aus diesem Grund hat sich der Düsseldorfer Kreis mit dem Thema befasst und einen Beschluss auf seiner Herbstsitzung am 24. und 25. November 2010 gefasst, in welchem Mindestanforderungen an Fachkunde und Unabhängigkeit der Beauftragten für den Datenschutz nach § 4 f Absatz 2 und Absatz 3 Bundesdatenschutzgesetz formuliert wurden (siehe unter Ziffer 20.4). Da es jedoch stets auf eine Betrachtung im Einzelfall (Struktur des Unternehmens, Art der Daten, et cetera) ankommt, handelt es sich lediglich um Mindestanforderungen, die nicht abschließend verstanden werden dürfen.

4. Datenschutz durch Technikgestaltung und Technikbewertung

4.1 Reorganisation von Berechtigungen im SAP

Wie wir bereits im 32. Jahresbericht, Ziffer 10.3, dargestellt haben, macht die Standortverlagerung der SAP-Systeme zu Dataport nach Hamburg eine grundlegende Überarbeitung der SAP-Konzepte erforderlich, die im Rahmen der Einführung von SAP durch das Projekt CHIPSMOBIL (vergleiche 26. Jahresbericht, Ziffer 13.3) erstellt worden waren.

Etwa 1 700 Benutzerinnen und Benutzer arbeiten derzeit mit SAP. Begonnen wurde im letzten Berichtsjahr mit der Überarbeitung des Berechtigungskonzepts, das mit dem Konzept „Kritische Berechtigungen“ zusammengeführt wurde (vergleiche 32. Jahresbericht, Ziffer 10.3). Es ist davon auszugehen, dass eine abschließende

Version des Berechtigungskonzepts in Kürze durch die Senatorin für Finanzen vorgelegt werden kann. Erstellung eines Konzepts heißt aber lange noch nicht Umsetzung. Diese Aufgabe ist im kommenden Jahr zu leisten. Und damit sie gelingt, müssen ausreichende personelle Ressourcen zur Verfügung stehen.

Weiterhin ist festzustellen, dass das Berechtigungskonzept nicht ohne Verweise auf andere weiterführende Konzepte, wie beispielsweise das IT-Rahmenkonzept, das Datenschutzkonzept, das Archivierungskonzept und das IT-Betriebskonzept, auskommen kann. Während das Archivierungskonzept noch gar nicht existiert, sind auch die anderen Konzepte aufgrund veränderter Infrastruktur und Rahmenbedingungen überarbeitungsbedürftig. Der bevorstehende Abschluss der Erstellung des Berechtigungskonzepts ist somit nur ein Baustein auf dem Weg zur Gewährleistung der Gesamtsicherheit des SAP-Systems. Wir wiederholen daher unsere Empfehlung aus dem Vorjahr, unverzüglich entsprechende Folgeprojekte aufzusetzen.

Unsere Anregungen und Hinweise zum Datenschutz wurden größtenteils im Berechtigungskonzept aufgenommen, beispielsweise Festlegungen zur datenschutzrechtlichen Verantwortung und Regelungen zur Einbeziehung der behördlichen Datenschutzbeauftragten in die Vorabkontrolle. Nach umfassenden Beratungen gibt es aus Sicht des Datenschutzes derzeit allerdings noch Klärungsbedarf in einigen Punkten.

Zum einen geht es hier um die Verwendung von sogenannten Sammelbenutzern, die nicht der üblichen Namenskonvention entsprechen und dessen Passwort mehreren Anwendern zur gleichzeitigen Nutzung bekannt ist. Zwar wird argumentiert, die Benutzer haben in der Regel ausschließlich Anzeigeberechtigungen auf den gleichen Datenbestand, dennoch aber halten wir die Verwendung von Sammelbenutzern grundsätzlich für nicht zulässig. Eine angemessene Kontrolle, welcher Mitarbeiter zu welchem Zeitpunkt auf Daten zugegriffen hat, scheint nicht gegeben. Wir erwarten in diesem Zusammenhang eine Darstellung des möglichen Zugriffs auf personenbezogene Daten sowie einen geeigneten Vorschlag dafür, wie zukünftig mit diesen Benutzern verfahren werden soll.

Regelungsbedarf besteht weiterhin bei der Vergabe von Berechtigungen im Qualitätssicherungssystem, in dem Programme, Berechtigungen und Szenarien getestet werden, bevor sie in das Produktivsystem transportiert werden. Bei diesem System handelt es sich um eine Kopie des Produktivsystems. In der Regel sollen im Qualitätssicherungssystem die gleichen Berechtigungen vorhanden sein wie im Produktivsystem; allerdings soll im Rahmen von Projekten ein größerer Berechtigungsumfang durch die Verwendung von SAP-Standardrollen an einzelne Projektmitglieder vergeben werden können. Somit kann es dazu kommen, dass Anwender auf dem Produktivsystem nur Einsicht in die Daten bekommen, die ihrer Bearbeitung unterliegen; im Qualitätssicherungssystem wird diese Zugriffskontrolle aber möglicherweise aufgehoben. Dieser Vorgehensweise können wir daher nicht grundsätzlich zustimmen. Aus Datenschutzsicht muss das Qualitätssicherungssystem aufgrund der Übereinstimmung der Daten mit dem Produktivsystem auch dem gleichen Schutzniveau unterliegen wie das Produktivsystem. Sollten tatsächlich umfangreichere Zugriffsberechtigungen für das Qualitätssicherungssystem vergeben werden müssen, so ist das nur mit Zustimmung der betroffenen Bereiche zulässig.

Darüber hinaus haben wir auf Risiken im Zusammenhang mit der Übermittlung von Benutzeranträgen per E-Mail verwiesen und die Restrisiken bezüglich des Verfahrens bei der Übersendung von Zugangskennungen benannt.

Abstimmungsbedarf gibt es derzeit auch noch bei den Löschfristen für die Benutzerstammsätze, die zunächst nicht gelöscht, sondern nur gesperrt werden. Hier fordert die Senatorin für Finanzen unter Berufung auf die Aufbewahrungsbestimmungen für Personalakten nach dem Bremischen Beamtengesetz eine Aufbewahrungsfrist von 30 Jahren. Wir halten in diesem Fall jedoch nicht das Bremische Beamtengesetz, sondern die allgemeinen datenschutzrechtlichen Vorschriften für anwendbar, wonach eine Löschung der Daten wesentlich früher erfolgen müsste.

Dringender Handlungsbedarf besteht insbesondere bei der Überarbeitung von technischen Berechtigungen, zum Beispiel den Batch-Input-Verfahren (mit Batch-Input lassen sich original SAP-Masken per Programm füllen und ausfüllen). Weiterhin offen ist die Reorganisation der Berechtigungen für den Support – also zum Beispiel SAP-Basis-Administratoren, Entwickler und Berater. Gerade in diesem Bereich sind sehr umfassende Berechtigungen vergeben worden.

Wir gehen derzeit davon aus, dass die noch offenen Punkte zügig geklärt werden können, erwarten aber, dass die noch ausstehenden Aufgaben, wie beispielsweise die Umsetzung des vor dem Abschluss stehenden Berechtigungskonzepts, die Überarbeitung der technischen Berechtigungen, die Reorganisation der Supportberechtigungen und die Anpassung der weiter aufgeführten und überarbeitungsbedürftigen Konzepte, in Folgeprojekten geleistet werden.

4.2 VIS – Zentrales System zur elektronischen Aktenführung

Als zentrales Dokumentenmangagementsystem wird im Land Bremen das System VISkompakt eingesetzt. Bereits im letzten Berichtsjahr (vergleiche 32. Jahresbericht, Ziffer 4.3) haben wir erste Unterlagen zur Beschreibung dieses Systems aus Datenschutzsicht bewertet und die nach dem Bremischen Datenschutzgesetz (BremDSG) erforderliche Verfahrensbeschreibung nebst Datenschutzkonzept von der Senatorin für Finanzen angefordert.

In diesem Berichtsjahr haben wir den ersten Entwurf des Sicherheitskonzepts zur elektronischen Akte der Freien Hansestadt Bremen (eAkte FHB) erhalten und nach gemeinsamer Beratung umfassend dazu Stellung genommen. Es handelt sich bei diesem Konzept nicht um die nach BremDSG zu erstellende Verfahrensbeschreibung. Im Gegensatz zu den nach § 7 BremDSG vorgegebenen Kontrollzielen, bezieht sich dieses Dokument auf die Schutzziele nach dem Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI-Grundschutz). Dabei kommen wir in unserer datenschutzrechtlichen Bewertung des Schutzbedarfs zu dem Ergebnis, dass der Schutzbedarf höher anzusiedeln ist. Hieraus erfolgt die Notwendigkeit zur Überarbeitung der erforderlichen Maßnahmen zur Gewährleistung des Schutzniveaus. Denn wie wir bereits im 32. Jahresbericht unter Ziffer 5.2 berichtet haben, soll VISkompakt unter anderem auch für das Projekt „Stopp der Jugendgewalt“ eingesetzt werden, in dem sehr sensible personenbezogene Daten verarbeitet werden. Insofern erwarten wir Ergänzungen zu den Maßnahmen für die Sicherstellung der Schutzziele sowie zu der vorliegenden Gefährdungsübersicht.

Insgesamt fällt auf, dass im vorliegenden Sicherheitskonzept an vielen Stellen auf weitere, uns nicht bekannte Konzepte und Untersuchungen verwiesen wird. Dies macht die Einordnung des vorliegenden Konzepts in die Gesamtdokumentation schwierig. Eine abschließende Bewertung ist derzeit aufgrund fehlender Angaben nicht möglich.

Die Senatorin für Finanzen unterscheidet in die zwei Verantwortungsbereiche eAkte-system und eAkte-Büro. Mit eAkte-system ist die zentrale System-Infrastruktur, der Bereich der Administration im VISkompetence Center sowie das IT-Verfahren selbst gemeint. Der Bereich eAkte-büro umfasst die VIS-Arbeitsplätze in den einzelnen Dienststellen, die administrativen Aufgaben in den Dienststellen sowie die Berechtigungsvergabe und Bearbeitung der Daten in den Mandanten.

Als Betreiberin und somit verantwortliche Stelle für eAkte-system wird die Senatorin für Finanzen genannt. Es ist daher darauf hinzuwirken, dass nach § 7 BremDSG die beziehungsweise der behördliche Datenschutzbeauftragte der verantwortlichen Stelle beteiligt wird. Unklar ist, welche Kontrollmaßnahmen und Genehmigungsprozesse für VIS festgelegt worden sind und in welcher Organisationseinheit bei der Senatorin für Finanzen das Sicherheitsmanagement für das IT-Verfahren eAkte angesiedelt ist.

Als Einheiten für Verantwortungsbereiche in eAkte-büro werden im VIS einzelne Ressorts einem Mandanten zugeordnet. Diese Zuordnung halten wir für zu pauschal und nicht zulässig. Es ist erforderlich, dass einzelne Dienststellen und gegebenenfalls sogar einzelne Projekte getrennte Mandanten erhalten können, da sonst die Zugriffskontrolle für die einzelne verantwortliche Stelle nicht umgesetzt und gewährleistet werden kann. Zu beachten ist in diesem Zusammenhang weiterhin das Trennungsgebot, wonach es unter bestimmten Bedingungen unzulässig sein kann, bestimmte Daten gemeinsam in einem Mandanten zu speichern. Außerdem kann es zu datenschutzrechtlichen Problemen kommen, wenn zwischen Ressorts die Verantwortlichkeiten wechseln. Die Dienststellen, die bereits VISkompakt einsetzen, sollten durch die Senatorin für Finanzen informiert werden, dass durch die verantwortlichen Dienststellen geeignete Datenschutzkonzepte für die festgelegten Verantwortungsbereiche zu erstellen sind. Eine detaillierte Stellungnahme zu den Berechtigungen und der Mandanteneinteilung ist uns allerdings erst möglich, wenn das vollständige Rechte- und Rollenkonzept vorliegt, das neben den vorge-

nannten Regelungen insbesondere auch die Aufgabenverteilung der Administratorinnen und Administratoren der auftragnehmenden und der verantwortlichen Stellen darstellen muss. Diese Problematiken sind zentral und müssen daher umgehend geklärt werden.

Derzeit ist unklar, welche Zugriffsmöglichkeiten die Administratorinnen und Administratoren auf den verschiedenen Infrastrukturebenen haben. Es muss daher ein Administrationskonzept erstellt werden, das die möglichen Zugriffe auf Betriebssystemebene, auf Datenbankebene sowie auf Anwendungsebene im VIS beschreibt. Weiterhin müssen die revisionssicheren Protokollierungen dieser Zugriffe beschrieben werden. Es muss weiterhin sichergestellt sein, dass grundsätzlich nur die berechtigten Administratorinnen und Administratoren Zugriff erlangen.

Da im System VISkompakt auch sehr sensible personenbezogene Daten bearbeitet werden sollen, halten wir eine Verschlüsselung der Daten auf Betriebssystemebene für erforderlich. Weiterhin sind zahlreiche Fragen zu den einzelnen Anlagen des Sicherheitskonzepts offen, deren Beantwortung derzeit noch aussteht.

Die Senatorin für Finanzen bearbeitet derzeit unsere Anregungen und Hinweise zum Datenschutz und kündigte an, Anfang des Jahres 2011 konsolidierte Unterlagen vorzulegen.

4.3 Administrativer Zugang am Dataport-Standort Bremen

Ein Thema, das uns nun schon im dritten Jahr begleitet (vergleiche 31. Jahresbericht, Ziffer 6.4 und 32. Jahresbericht, Ziffer 4.2), ist die Einrichtung einer sogenannten Admin-Area – eines einheitlichen und revisionssicheren Weges zur Durchführung von Administrationstätigkeiten – für bremische Verfahren.

Bereits vor zwei Jahren leitete die Senatorin für Finanzen uns eine Dokumentation aus einem Dataport-internen Projekt zu, auf dessen Grundlage eine gesonderte Variante für den Standort Bremen aufgesetzt worden war. Die offenen Fragestellungen, die sich aus diesen Unterlagen ergaben und zu denen beispielsweise die Protokollierung und Revision sicherheitskritischer administrativer Tätigkeiten gehört, konnten bisher nicht geklärt werden.

In der Stellungnahme des Senats zu unserem 31. Jahresbericht wurde uns die Vorlage einer konsolidierten Dokumentation angekündigt. Auf Nachfrage übersandte die Senatorin für Finanzen uns in diesem Berichtsjahr die Fortschreibung des Konzepts zur Einführung der oben beschriebenen Admin-Area. Eine Stellungnahme unsererseits wird allerdings erst dann erfolgen, wenn die nach dem Bremischen Datenschutzgesetz vorgesehene Vorabkontrolle durch die Senatorin für Finanzen stattgefunden hat und eine Anwendbarkeit des Konzepts für Bremen sichergestellt ist. Zwischenzeitlich teilte uns die Senatorin für Finanzen mit, dass mit einer Aufnahme des Betriebs voraussichtlich im zweiten Quartal 2011 zu rechnen ist.

4.4 Faktische Wahrnehmung datenschutzrechtlicher Verantwortung in vernetzten IT-Systemen

Umgangssprachlich bezeichnet Verantwortung die Möglichkeit, für die Folgen eigener oder fremder Handlungen Rechenschaft abzulegen. Verantwortung drückt sich danach darin aus, bereit und fähig zu sein, später Antwort auf mögliche Fragen zu deren Folgen zu geben. Eine Grundvoraussetzung hierfür ist die Fähigkeit zur bewussten Entscheidung. Eine Verantwortung zieht immer eine Verantwortlichkeit nach sich, das heißt, dafür Sorge zu tragen, dass die Entwicklung des Verantwortungsbereichs im gewünschten Sinne verläuft. Verantwortung im datenschutzrechtlichen Sinne bezeichnet das Einstehen-Müssen für einen datenschutzgerechten Zustand. Sie wird nach den Datenschutzgesetzen derjenigen Stelle zugesprochen, die personenbezogene Daten für sich selbst verarbeitet oder dies durch andere im Auftrag vornehmen lässt.

Es stellt sich die Frage, ob es angesichts der schwindenden faktischen Steuerungsmöglichkeiten verantwortlicher Stellen noch legitim ist, diesen die datenschutzrechtliche Verantwortung zu belassen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihren Eckpunkten für ein modernes Datenschutzrecht für das 21. Jahrhundert (vergleiche Ziffer 1.4 dieses Berichts) gefordert, das Konzept der Zuweisung von Verantwortlichkeiten neu zu fassen. Wir schlagen beispielsweise vor allem für die Fälle der Beteiligung mehrerer Stellen an der Datenverarbeitung die Normierung des Prinzips der nachhaltigen Verantwortlichkeit

(„Accountability“) vor. Danach wäre jeweils die Stelle datenschutzrechtlich verantwortlich, die in tatsächlicher Hinsicht über Mittel und Zwecke der Datenverarbeitung verantwortlich bestimmen kann.

Ein exemplarisches Beispiel für den Steuerungsverlust der datenschutzrechtlich verantwortlichen Stellen ist das Cloud Computing (Rechnen in der Wolke, vergleiche Ziffer 4.5 dieses Berichts). Hierunter wird im Allgemeinen das Auslagern von Daten und Arbeitsprozessen über ein Netz auf andere Server, die von Unternehmen angeboten werden, bezeichnet.

Auch die folgenden Beispiele aus der bremischen Verwaltung (Verwaltungs-PC, Ziffer 4.4.1), aus dem Bereich der Gesundheitsverwaltung und neuer Technologien (Ziffer 4.4.2) und der Internettelefonie (Ziffer 4.4.3) zeigen in sehr unterschiedlichen Szenarien, wie schwierig die faktische Wahrnehmung der datenschutzrechtlichen Kontrolle der Verarbeitungsprozesse werden kann. Anwenderinnen und Anwender wissen nicht mehr, wo sich ihre Daten rein physikalisch befinden, wie sie durch wen verarbeitet werden, wie sicher sie tatsächlich gegen missbräuchliche Zugriffe geschützt sind und bei Grenzüberschreitungen wissen sie nicht, welcher datenschutzrechtliche Standard überhaupt gilt. Nach deutschem Datenschutzrecht bleibt die Verantwortung immer bei der verantwortlichen Stelle. Solange es aber keine gesetzliche Neuregelung gibt, verbleibt die datenschutzrechtliche Verantwortung bei der „verantwortlichen Stelle“ im Sinne der Datenschutzgesetze, also bei der Stelle, die „personenbezogene Daten“ für sich selbst verarbeitet oder dies durch andere im Auftrag vornehmen lässt.

4.4.1 Verwaltungs-PC

Die Freie Hansestadt Bremen (FHB) strebt grundsätzlich eine Vereinheitlichung des IT-Supports (Informationstechnik-Dienstleister) und eine weiterführende Standardisierung der IT-Infrastruktur durch Verlagerung von IT-Betriebsaufgaben auf die Anstalt öffentlichen Rechts Dataport als zentralem Dienstleister der FHB an. Laut Senatsbeschluss aus dem Jahr 2007 soll die Konzeption „durch Einführung eines User Helpdesks (eines zentralen Informationsdienstes zur Unterstützung von Anwendern) und softwarespezifischer netzgestützter Anwenderbetreuung in Zusammenarbeit mit Dataport entwickelt und umgesetzt“ werden. Dataport wurde deshalb von der Senatorin für Finanzen mit der Erstellung eines Konzepts, das den Verwaltungsarbeitsplatz in seiner technischen Ausprägung sowie die Serviceleistungen bei einem zentralen Betrieb durch Dataport beschreibt, beauftragt.

Durch die Zentralisierung von IT-Abläufen entstehen neue Risiken, die datenschutzrechtlich bewertet und in der Gestaltung der technischen Infrastruktur berücksichtigt werden müssen.

Hierzu sind die Auswirkungen auf den Schutz der Daten der Bürgerinnen und Bürger und sich daraus möglicherweise ergebende neue Anforderungen an die Systeme, systematisch im Hinblick auf die Gestaltung einer datenschutzkonformen IT-Infrastruktur zu analysieren. Darüber hinaus entstehen durch die Nutzung der Infrastruktur neue Daten. Diese sind zu identifizieren und datenschutzgerecht zu behandeln. Auch durch die Zentralisierung entstehende technische Probleme der Datensicherheit müssen identifiziert und behoben werden. In Bezug auf zentrale Verfahren und Dienstleistungen entsteht außerdem eine neue, sich nicht im direkten sozialen Kontext mit den für die Daten verantwortlichen Dienststellen befindende Administrationsebene. Die Eingriffstiefe dieser zentralen Ebene muss definiert werden und kontrollierbar sein. Die hohe Abstraktionsebene erfordert „objektive Messverfahren“ für die IT-Sicherheit. Dieses sieht Dataport in seinem IT-Sicherheits- und Datenschutz-Managementhandbuch durch Schaffung von Kennzahlen (KPI – Key Performance Indicators, zu Deutsch Leistungskennzahl) zur Messung des Erfüllungsgrads von Prozessen oder kritischer Erfolgsfaktoren vor, deren genaue Definition hinsichtlich der Qualitätskriterien noch nicht vorliegt.

Die datenschutzrechtliche Verantwortung der speichernden Stellen muss innerhalb der zentralisierten Strukturen weiterhin faktisch wahrnehmbar sein. Nach der geltenden Rechtslage ist die für die Datenverarbeitung verantwortliche Stelle jede Stelle, die personenbezogene Daten für sich selbst verarbeitet oder dies durch andere im Auftrag vornehmen lässt. Diese verantwortliche Stelle müsste bei der Verarbeitung personenbezogener Daten ihr Netz abschotten und die Kontrolle über die Verarbeitung der Daten ausüben, die außerhalb ihres Netzes erfolgt. Hierbei bildet die Schutzbedürftigkeit der in den einzelnen Verarbeitungsprozessen verar-

beiteten personenbezogenen Daten die Grundlage zur Bewertung der erforderlichen Stärke der Maßnahmen. Die Ausübung dieser Kontrolle ist durch die Komplexität der Infrastruktur und der Zugangsmöglichkeiten in den vernetzten IT-Systemen sehr erschwert.

Neben den bereits in unserem 30. Jahresbericht unter Ziffer 6.2 dargestellten Anforderungen zur Nutzung von Fernwartungssoftware im Rahmen eines zentralen Servicedesk für Dataport Bremen erweitern sich die datenschutzrechtlichen Fragestellungen auf die gesamte Infrastrukturkette vom Endgerät über die Netzwerke bis zum Rechenzentrum. In den Ausführungen zum IT-Sicherheitsmanagement im Land Bremen ist bereits deutlich geworden, wie eng der Datenschutzprozess mit dem IT-Sicherheitsprozess verzahnt ist (vergleiche 32. Jahresbericht, Ziffer 4.1). Datenschutzrechtliche Anforderungen müssen im Rahmen angemessener IT-Sicherheitsmaßnahmen umgesetzt werden.

In der Dataport-Datenschutzleitlinie vom 9. Juli 2010, Version 1, verpflichtet sich Dataport zu einer den Landesdatenschutzgesetzen konformen Datenverarbeitung und weist gleichzeitig auf die Verantwortlichkeit des Auftraggebers für die von ihm in Auftrag gegebene Datenverarbeitung hin. Wir haben deshalb im Rahmen der Arbeitsgruppe zur Basisinfrastruktur des Teilprojekts zur Einführung des Verwaltungs-PC „IT-Querschitt“ folgende Anforderungen formuliert:

Es müssen datenschutzrechtliche Steuerungsinstrumente innerhalb des Standardisierungsservices, der die ganze Infrastrukturkette vom Endgerät über die Netzwerke bis zum Rechenzentrum umfasst, festgelegt werden und die Modalitäten ihrer Durchführung beschrieben werden. Es ist dabei in Bezug auf Organisation und Technik zu beschreiben, wie die datenschutzrechtlichen Verantwortlichkeiten der Ressorts wahrgenommen werden müssen. Für den Ausbau der Standardisierung fordert das Gesamtkonzept Verwaltungsarbeitsplatz der FHB, Version 1.0 vom 12. Dezember 2009, Klarheit und Transparenz von Rollen, Verantwortung und Kompetenz zur Planung, Umsetzung und Überwachung der Sicherheitsinfrastruktur. Es sind danach schriftliche Weisungen zu technischen und organisatorischen Maßnahmen bezüglich der datenschutzrechtlichen Konformität der Auftragsdatenverarbeitung sowie Sicherheitskonzepte zu erstellen. Die Dataport-Leitlinie fordert dies auch für Fachverfahren. Weiterhin ist in dem Dokument festgelegt, dass die Sicherheitsmaßnahmen vertraglich vereinbart werden. Deshalb sind vertragliche Verankerungen von Sicherheitsmaßnamen notwendig. Die Maßnahmen müssen Personaldaten und Daten der Bürgerinnen und Bürger schützen. Weiterhin halten wir eine Bestandsaufnahme der gesamten IT-Infrastruktur sowie der Verfahren der Ressorts und eine Beschreibung der IT-Sicherheitsmanagementprozesse für die IT der Ressorts, die Erstellung eines Administrationskonzepts, insbesondere unter Berücksichtigung der für die Betriebsorganisation geplanten Tools (Werkzeuge) sowie die Erstellung von Detailkonzepten zur Nutzung administrativer Tools, die Konfiguration der Schnittstellen zum Bremischen Verwaltungsnetz, die Definition von Gruppenrichtlinien auf den verschiedenen Ebenen und Revisionsverfahren für kritische Berechtigungen innerhalb der Gesamtstruktur (inklusive der Nutzung administrativer Tools), für erforderlich.

Zur Gewährleistung eines datenschutzgerechten Betriebs des Verwaltungs-PC halten wir zusammenfassend die Schaffung folgender Voraussetzungen für notwendig:

— Die Beschreibung und Berücksichtigung grundsätzlicher Auswirkung der Zentralisierung auf Bürger- und Beschäftigtendaten.

— Die klare Definition von Verantwortlichkeiten unter Berücksichtigung der geltenden Rechtslage und der zentralisierten IT-Strukturen und den Aufbau eines entsprechenden Sicherheitsmanagements.

— Die Erstellung systematisch aufgebauter und inhaltlich bis auf die operative Ebene eindeutiger IT-Sicherheitsdokumente, die auf einer Analyse der bremischen Infrastruktur aufsetzen.

— Eine datenschutzkonforme Umsetzung der mit der Entwicklung des Bremer Landesnetzes zusammenhängenden Projekte, wie beispielsweise der Aufbau eines sicheren Active Directory (Verzeichnisdienst) und das Sicherheitsmanagement lokaler und dezentraler Netzinfrastrukturen. Dabei sind insbesondere Konzepte für die Organisation, die Systemadministration und die Herstellung der Revisionssicherheit zu entwickeln.

— Die Erweiterung des Budgets um Kosten der Sicherheit des Betriebs als Teilaspekt des Gesamtprojekts.

4.4.2 Sichere Onlinedatenübermittlung von Abrechnungsdaten durch Ärzte und Psychotherapeuten

Ärztinnen und Ärzte sowie Psychotherapeutinnen und Psychotherapeuten müssen künftig patientenbezogene Daten an die Kassenärztliche Vereinigung Bremen (KVHB) zu Abrechnungszwecken online übermitteln. Gemäß § 78 a Zehntes Sozialgesetzbuch (SGB X) sind bei der Verarbeitung von Sozialdaten die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführungen der Vorschriften des SGB – insbesondere die in der Anlage zu § 78 a SGB X genannten Anforderungen – zu gewährleisten. Demnach sind solche Maßnahmen zu treffen, die je nach Art der zu schützenden Sozialdaten oder der Kategorie von Sozialdaten sicherstellen, dass ausschließlich Berechtigte auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass Sozialdaten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle). Die Sensibilität und Schutzbedürftigkeit der Daten, die zwischen psychotherapeutischen und ärztlichen Praxen und der Kassenärztlichen Vereinigung übertragen werden, erfordert, dass die eingesetzten Sicherheitsmechanismen der besonderen Schutzwürdigkeit von Patientendaten entsprechen.

Die Kassenärztliche Bundesvereinigung empfiehlt zum Zweck der leitungsgebundenen elektronischen Abrechnung die Nutzung der medizinischen Netz- und Diensteinfrastruktur der kassenärztlichen Bundesvereinigung KV-SafeNet. Kern dieser Kommunikationslösung ist ein Hardware-VPN (Virtuelles Privates Netz – eine Netzinfrastruktur, bei der Komponenten eines privaten Netzes über ein öffentliches Netz wie dem Internet miteinander kommunizieren, wobei sie die Illusion besitzen, das Netz zu ihrer alleinigen Verfügung zu haben), das unter Sicherheitsaspekten grundsätzlich als die zuverlässigste Lösung gilt. Wir haben diese Lösung und diejenige einer qualitativ hochwertigen Software-VPN-Lösung als datenschutzrechtlich angemessen bewertet.

Die KVHB hat uns hierzu im Sommer des Berichtsjahrs einige technische Lösungsmodelle vorgestellt, die wir hinsichtlich ausgewählter Sicherheitsaspekte der Übertragungssicherheit bewertet haben. Dazu gehörte unter anderem die Sicherheit des Authentifizierungsverfahrens und die Manipulierbarkeit und/oder Fehleranfälligkeit der Komponenten. Der Übertragungsweg ist jedoch nur ein Teil der Datensicherheit. Das Schutzniveau ist immer in Bezug auf den Gesamtkontext und das Zusammenwirken aller technischen und organisatorischen Maßnahmen zu bewerten. Dabei sind die Sicherheit des lokalen Praxissystems, die Absicherung der externen Verbindungen gegenüber dem Internet, der Schutz der Vertraulichkeit und Integrität der Daten auf dem Transportweg und die Sicherheit der Systeme der Kassenärztlichen Vereinigung zu beachten.

In Bezug auf den Einsatz der Hardware-VPN-Lösung zum Anschluss der Praxen haben wir noch datenschutztechnische Fragen an die KVHB gerichtet, die sich insbesondere auf die Kontrolle der für den Betrieb und Support von der Kassenärztlichen Bundesvereinigung zertifizierten Provider beziehen. Hierzu gehören die Sicherstellung des Sicherheitsmanagements der beauftragten Firmen (Provider) und deren Kontrolle, insbesondere die Dokumentation von Maßnahmen, um fehlerhafte oder unbefugte Administration der Komponenten zu verhindern und die Sicherheitsmaßnahmen in den Zugangsnetzen der Provider zu kontrollieren. Die Rahmenrichtlinie KV-SafeNet (Version 3.0 vom 6. März 2009) schließt eine Gewährleistung bezüglich der IT-Sicherheit des Zugangsnetzes der beauftragten Firmen durch die Kassenärztliche Vereinigung aus.

Datenschutzrechtlich verantwortlich bleiben die einzelnen Praxen. Diese haben auch laut der genannten Richtlinie ein Kontrollrecht. Um dieses wahrzunehmen, müssten die Praxen selbst die Sicherheit der Provider überprüfen. Dies wird im Einzelfall kaum möglich sein. Die Praxen bewegen sich datenschutzrechtlich zwischen wahrzunehmender Verantwortung hinsichtlich der Gewährleistung der ärztlichen Schweigepflicht und einem faktischen Kontrollverlust durch die gesetzlich vorgeschriebene Nutzung komplexer Technologien.

Wir haben deshalb die KVHB aufgefordert, für den gesamten Geschäftsprozess datenschutz- und datensicherheitsbezogene Steuerungsmechanismen festzulegen und ein geeignetes Revisionskonzept vorzulegen.

4.4.3 IP-Telefonie mit sensiblen Daten – Skype

An uns ist die Anfrage gestellt worden, ob das Angebot über Internettelefonie (Voice over IP) des in Luxemburg ansässigen Anbieters Skype ausreichende technische und organisatorische Sicherheitsmaßnahmen bietet, um Daten aus dem medizinischen Bereich übermitteln zu können.

Auch wenn das Unternehmen im Land Bremen seinen Sitz hat, gilt für die Datenverarbeitung im Bereich der Telekommunikation die Besonderheit, dass die Datenschutzkontrolle nach dem Bundesdatenschutzgesetz durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) ausgeübt wird. Deshalb konnten wir den Anfragenden zum Einsatz von Skype nur Kriterien nennen, nach denen die verantwortlichen Stellen die Möglichkeit eines datenschutzgerechten Einsatzes des Systems prüfen können. Die verantwortlichen Stellen haben sicherzustellen, dass sie ein datenschutzgerechtes Verfahren einsetzen. Im öffentlichen wie im nicht öffentlichen Bereich sind Vorabkontrollen in Bezug auf die durch die Nutzung des Verfahrens möglichen Gefahren für die Betroffenen durchzuführen. Im öffentlichen Bereich muss die verantwortliche Stelle das Ergebnis der Vorabkontrolle der oder dem behördlichen Datenschutzbeauftragten zur Prüfung zuleiten. Im nicht-öffentlichen Bereich ist die oder der Beauftragte für den Datenschutz nach Empfang der gesetzlich vorgesehenen Übersicht, die auch die Beschreibung der technischen und organisatorischen Maßnahmen enthält, selbst für die Vorabkontrolle zuständig. In Zweifelsfällen kann sich die oder der Datenschutzbeauftragte an den BfDI wenden. Für diese Bewertung der Nutzung von Skype müssen verschiedene Sicherheitsebenen betrachtet werden.

Bezüglich des Telekommunikationsanbieters Skype gilt, dass die Unternehmen Skype Software S.a.r.l. und/oder Skype Communications S.a.r.l. ihren Geschäftssitz in Luxemburg haben. Sie haben für die Verarbeitung ihrer personenbezogenen Daten Datenschutzrichtlinien erstellt, die im Internet veröffentlicht sind. Datenschutzrechtlich ergibt sich dadurch das grundsätzliche Problem, dass die Einhaltung dieser Richtlinien und die Umsetzung der dargestellten Sicherheitsmethoden durch die verantwortlichen Stellen nicht direkt geprüft werden können. Den Datenschutzbeauftragten vor Ort fehlen bereits prüfbare Dokumentationen.

Geht die verantwortliche Stelle davon aus, dass die Datenschutzrichtlinien von Skype eine zuverlässige Umsetzung erwarten lassen, ist der Inhalt der Richtlinien im nächsten Schritt dahingehend zu prüfen, ob die Qualität den Anforderungen der Datenübermittlung sensibler personenbezogener Gesundheitsdaten gerecht wird. Zu beachten ist dabei, dass die Verarbeitung besonderer Arten personenbezogener Daten gemäß § 3 Absatz 9 Bundesdatenschutzgesetz (BDSG) ein hohes Schutzniveau erfordert.

Grundsätzliche Fragen an den Anbieter von Voice over IP müssten sich auf die Gewährleistung der Sicherheit der Verschlüsselung der Kommunikationsinhalte (besonders unter dem Aspekt der Zertifikatsvergabe durch den Anbieter selbst), die Sicherheit des Authentifizierungsverfahrens, den möglichen Zugriff auf Kommunikationsinhalte durch Skype und die Inhalte von Ereignisprotokolldateien (Logfiles) und den Zugriff darauf beziehen. Aus der Datenschutzrichtlinie des Anbieters lässt sich unter anderem entnehmen, dass Skype externe, nicht näher benannte Diensteanbieter zur Sammlung und Verwertung personenbezogener Nutzerdaten beauftragt, dass Skype Nutzerdaten und Verkehrsdaten ohne Benennung von Gründen („wenn dies nötig ist“) weitergibt, dass eine Sprachnachricht gegebenenfalls an ein anderes Unternehmen übermittelt und dort in eine Textnachricht umgewandelt wird, dass Analysten dann auf diese Textnachricht zugreifen können und dass Informationen gegebenenfalls in Ländern aufbewahrt und verarbeitet werden, die sich außerhalb der Europäischen Union befinden.

Bei der verantwortlichen Stelle ist zu beachten, dass diese, falls sie sich entscheidet, Skype zu nutzen, verpflichtet ist, wirksame technische und organisatorische Maßnahmen zu ergreifen, um den Schutz der personenbezogenen Daten zu gewährleisten. Grundsätzlich ist davon auszugehen, dass die über Voice over IP übermittelten Sprachinformationen den gleichen Risiken unterliegen wie herkömmliche internetbasierte Applikationen. Sie können also abgehört, entwendet oder manipuliert werden. Es ist deshalb erforderlich, die Sicherheitsaspekte, die auch für die übrige IT-Infrastruktur gelten, zu berücksichtigen. Als grundsätzliche Erfordernisse können unter anderem die Verschlüsselung der Datenpakete in eigener Verantwortung, der Einsatz von Virenschutz-Software, die Absicherung der WLAN

(drahtlose lokale Netzwerke), die Nutzung von IDS (Intrusion Detection System, zu Deutsch etwa Systeme zur Erkennung von Angriffen, die gegen ein Computersystem oder Computernetz gerichtet sind) und Firewallsystemen (eine Software zur Beschränkung von Netzwerkzugriffen) betrachtet werden.

Die nationale Kommission für den Datenschutz aus Luxemburg hat uns mitgeteilt, dass sie die Sicherheitsmaßnahmen von Skype noch nicht im Detail bewertet hat, dies aber in absehbarer Zeit tun und uns diesbezüglich auf dem Laufenden halten wird.

4.5 Cloud-Computing

Mit „Rechnen in der Wolke" kann man den Begriff Cloud Computing übersetzen. Umgangssprachlich werden die Daten in der Cloud, also der Wolke, verarbeitet. Die (technische) Idee, die dahintersteckt, ist, dass man sich schnell benötigte Rechenkapazität, Speicherplatz oder die neueste Version der einzusetzenden Software besorgen kann, aus einem abstrakten Gebilde, einer Wolke, etwa für ein Großprojekt, bei dem große Datenbestände einmalig zusammengeführt werden müssen, vorinstalliert, vorkonfiguriert, ganz nach dem Wunsch der Nutzerin oder des Nutzers, einfach von einem Anbieter die notwendige Menge an Rechenkapazität einkaufen, über das Internet, wenn es nicht reicht, einfach noch etwas dazumieten. Nach dem Ende des Projekts werden die Ressourcen einfach wieder freigegeben. Anwender des Cloud Computing freuen sich. Sie erhalten eine hohe Flexibilität. Können dabei aber Investitionen und den Ausbau eigener Infrastrukturen klein halten. Anbieter wie Rechenzentren oder andere Dienstleister aus dem Umfeld der Informationstechnik freuen sich, können sie doch so ihre – oft zwingend vorzuhaltenden – Überkapazitäten betriebswirtschaftlich nutzen.

Es gibt Clouds, die nur einer geschlossenen Nutzergruppe zur Verfügung stehen, sogenannte Private Clouds. Und es gibt Public Clouds, was mit „öffentliche Wolken" zu übersetzen ist und Clouds beschreibt, die nahezu von allen genutzt werden können. Beide genannten Formen können auch als Mischform genutzt werden; selbstverständlich auch in Verbindung mit der eigenen Informationstechnik-Infrastruktur der Nutzerin oder des Nutzers, maximale Flexibilität, geringe Kosten.

Für die Datensicherheit, und ganz besonders auch aus Sicht des Datenschutzes, ist das gar nicht unproblematisch. Gerade bei den Public Clouds sind die Anbieter meist weltumspannend aktive Informationstechnikunternehmen, die eben auch weltweit verteilt Rechenzentren betreiben oder nutzen. Dabei kann sich die Nutzerin oder der Nutzer eigentlich nie sicher sein, wo auf der Welt ihre oder seine Daten aktuell gespeichert sind, auf welchen Maschinen die Daten momentan verarbeitet werden. Auf welchem Computer, in welchem Rechenzentrum, in welchem Unternehmen welcher wirtschaftlichen Lage, in welchem Staat und politischem System, auf welchem Kontinent – alles dies bleibt im undurchdringlichen Nebel der Cloud. Und damit auch die Frage, wer (unbefugt) Zugriff auf die Daten hat. Sei es beim Transport von oder zur Cloud, bei der Speicherung und Verarbeitung oder auch beim Verschieben der Daten innerhalb der Cloud, das oft ohne Wissen der Anwenderin oder des Anwenders geschieht. Anbieter von Cloud-Dienstleistungen beschaffen sich bei Engpässen auch kurzfristig Rechenleistung bei anderen Anbietern und verschieben die Datenverarbeitung schnell und technisch problemlos dahin. Mit einem Mausklick auf die andere Seite der Erde. Die Nutzerin oder der Nutzer hat in der Regel keinerlei Kontroll- und Einflussmöglichkeit darauf. Dabei spielt nach dem Datenschutzrecht der Ort der Datenverarbeitung eine entscheidende Rolle: vielleicht nicht innerhalb der Europäischen Union (EU), wo es angeglichene Niveaus (im Sinne von Qualität) gibt, wohl aber dann, wenn es darüber hinaus geht. Die datenschutzbezogenen Rechte der Betroffenen können aber prinzipiell nicht anders sein als im Inland, bloß weil die Daten gerade in einem Staat außerhalb der EU verarbeitet werden. Und auch die Qualität des technischen und rechtlichen Schutzes für die personenbezogenen Daten darf dadurch nicht geringer werden.

Zentrale „technische" Probleme des Cloud Computing sind also die Integrität (Unverletztheit) und vor allem auch die Vertraulichkeit der verarbeiteten (personenbezogenen) Daten. Die Daten müssen vor Zugriffen Dritter geschützt sein. Dabei ist es egal, ob es sich dabei um „lesende" Zugriffe oder um Zugriffe handelt, bei denen Daten verändert werden. Und zwar während der Nutzung der Cloud, also der Gültigkeit des Vertrages zwischen Anbieter und Nutzerinnen und Nutzern, und

darüber hinaus. Dann müssen die Daten unumkehrbar und vor allem vollständig und prüfbar gelöscht werden. Egal wo sie auf der Welt „gelegen“ haben.

Datenschutzrechtlich verantwortlich für die Datenverarbeitung in der Cloud sind in der Regel die Nutzerinnen und Nutzer der Cloud-Dienstleistungen. Das Bremische Datenschutzgesetz und das Bundesdatenschutzgesetz sprechen dabei von der „Verantwortlichen Stelle“. Die Verantwortliche Stelle ist gesetzlich verpflichtet, zu gewährleisten, dass die gesetzlichen Vorgaben über den Datenschutz eingehalten werden. Dazu muss sie Auftragnehmer, also Anbieter von Cloud Computing, sorgfältig und unter Berücksichtigung der von ihnen getroffenen technischen und organisatorischen Maßnahmen zum Schutz der zu verarbeitenden personenbezogenen Daten auswählen. Und Datenverarbeiter müssen sich der Kontrolle der zuständigen Datenschutz-Aufsichtsbehörde unterwerfen. Das ist zwar vertraglich zu regeln, wird sich im Umfeld von Cloud Computing aber nur äußerst schwierig realisieren lassen.

Aus der Sicht des Datenschutzes lassen sich für die Verarbeitung personenbezogener Daten Clouds derzeit nur in geringem, klar definiertem Umfang nutzen. Nämlich dann, wenn Anbieter garantieren können, dass die Daten lediglich innerhalb der EU verarbeitet werden und die datenschutzrechtlichen Anforderungen im Hinblick auf die Qualität des Datenschutzes in vollem Umfang gewährleistet sind.

Im Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder wird derzeit eine Informationsbroschüre zum Thema „Cloud Computing und Datenschutz“ erarbeitet. Sobald diese fertig gestellt ist, werden wir diese Informationsschrift auf unserer Internetseite veröffentlichen.

5. Inneres

5.1 E-Mail-Anfrage des Landeskriminalamts Bremen

Das Landeskriminalamt (LKA) Bremen hatte eine Person, die eine Internetseite mit einem Forum betreibt, per E-Mail angeschrieben und um Auskunft der personenbezogenen Daten einer anderen Person, die das Internetforum nutzt, gebeten. Hintergrund dieser E-Mail-Anfrage des LKA Bremen waren konkrete polizeiliche Ermittlungen im Internet. Das LKA Bremen fragte nach den Nutzungsdaten einer Zeugin beziehungsweise eines Zeugen. Die das Internetforum betreibende Person war sich unsicher, ob diese E-Mail-Anfrage tatsächlich vom LKA Bremen stamme und ob dieses polizeiliche Verhalten datenschutzrechtlich zulässig sei.

Eine derartige E-Mail-Anfrage des LKA Bremen auf unverschlüsseltem Weg ist wegen des Gehalts an personenbezogenen Daten datenschutzrechtlich unzulässig. Die Polizei Bremen hat zugesagt, künftig kriminalpolizeiliche Anfragen mit personenbezogenen Daten grundsätzlich auf dem Postweg oder, in dringenden Fällen, per Fax vorzunehmen.

5.2 E-Mail-Irrläufer der Polizei Bremen

In diesem Jahr haben wir die Polizei auf einige Fälle hingewiesen, in denen elektronische Nachrichten versehentlich an einen unberechtigten Empfängerkreis gesendet worden sind. Häufigste Ursache sind Unachtsamkeiten bei der Auswahl der Adressaten aus der globalen Adressliste des bremischen Verwaltungsnetzes (BVN). Die Polizei Bremen hat ihre Mitarbeiterinnen und Mitarbeiter auf diese Fehlerquelle hingewiesen und sie aufgefordert, bei der Adresseingabe besonders darauf zu achten, dass nur die gewünschten und damit korrekten Empfängerinnen und Empfänger ausgewählt werden.

Zur Vermeidung von Fehleingaben hat die Polizei Bremen ihre Mitarbeiter darauf hingewiesen, dass das Adressbuch der Polizei Bremen als Standard voreingestellt werden kann und ein Zugriff auf das globale Adressverzeichnis dann nur im Bedarfsfall erfolgt.

Im Zusammenhang mit diesen Vorfällen machte die Polizeiführung ihre Mitarbeiterinnen und Mitarbeiter erneut auf die Mitteilung Nummer 10 des IT-Sicherheitsbeauftragten betreffend die Vertraulichkeit beim E-Mail-Versand aus Oktober 2009 aufmerksam. Diese Mitteilung beinhaltet die technischen Aspekte bei der Nutzung von E-Mail bei der Polizei Bremen, insbesondere die Regelungen zur Verschlüsselung und gegebenenfalls zur Verwendung der digitalen Signatur bei dem Versand von E-Mails an andere Behörden innerhalb des bremischen Verwaltungsnetzes, wie

zum Beispiel an die Staatsanwaltschaft oder an den Senator für Inneres und Sport und über das Internet. Die Beschäftigten wurden daneben nochmals auf die bestehenden Vorgaben des Bremischen Datenschutzgesetzes, auf polizeiinterne Regelungen zur Sicherheit und auf Dienstanweisungen hingewiesen und über die Risiken und Gefahren bei der Nichteinhaltung der zwingend vorgegebenen Maßnahmen informiert.

5.3 Polizeikontrollen auf dem Autobahnparkplatz Krummhörens Kuhlen

Auf dem Autobahnparkplatz Krummhörens Kuhlen an der Bundesautobahn 1 in Richtung Hamburg und in der näheren Umgebung, wie zum Beispiel am Silbersee, werden von der Polizei Bremen Kontrollen zur Identitätsprüfung vorgenommen. Dabei werden insbesondere die Personalien und die Kraftfahrzeugkennzeichen erfasst. Uns erreichten Beschwerden von Bürgern, in denen vermutet wurde, dass die Polizei Homosexuelle diskriminiere. Die polizeiliche Kontrolle beziehe sich nur auf männliche Personen. Die Bürger fühlen sich in ihren Persönlichkeits- und Freiheitsrechten beeinträchtigt und fragten nach der datenschutzrechtlichen Zulässigkeit der Erhebung und Speicherung ihrer personenbezogenen Daten.

Die Polizei nimmt hier ihre Aufgabe zur Verhütung von Straftaten und Ordnungswidrigkeiten wahr. In der Vergangenheit wurden nach Auskunft der Polizei Bremen auf dem genannten Autobahnparkplatz Straftaten, wie zum Beispiel schwerer Raub, sexueller Missbrauch von Kindern, exhibitionistische Handlungen und Erregung öffentlichen Ärgernisses sowie Ordnungswidrigkeiten, wie die Belästigung der Allgemeinheit und grob anstößige und belästigende Handlungen, begangen. Schwerer Raub und sexueller Missbrauch von Kindern sind Straftaten von erheblicher Bedeutung. Ihr Vorliegen begründet die Annahme einer abstrakten Gefahrenlage. Sofern der Verdacht der Begehung dieser Straftaten beziehungsweise die Gefahr besteht, dass diese begangen werden, ist das polizeiliche Vorgehen datenschutzrechtlich zulässig. Aktuell befinden wir uns mit der Polizei Bremen noch in einem Informationsaustausch zur datenschutzrechtlichen Kontrolle des polizeilichen Vorgehens.

5.4 Auskunfts- und Löschungsbegehren betreffend ISA-Web und INPOL

Das bremische polizeiliche Informationssystem Strafanzeigen (ISA-Web) enthält personenbezogene Daten von Anzeigen erstattenden Personen und von angezeigten Personen, von beschuldigten beziehungsweise verdächtigen Personen, von Zeuginnen und Zeugen, Opfern und Hinweisgebern. Jede natürliche Person kann Auskunft aus ISA-Web und gegebenenfalls die Löschung der betreffenden Daten begehren.

Manchmal wird in diesem Zusammenhang eine Speicherung im Informationssystem der Polizei (INPOL) festgestellt. INPOL ist eine elektronische Datensammlung und -verarbeitung der Polizei auf Bundes- und Landesebene. Jedem Verbundteilnehmer (zum Beispiel dem Landeskriminalamt Bremen für das Bundesland Bremen) wird der Zugriff auf die in dieser Verbunddatei gespeicherten, personenbezogenen Daten gewährt. Bei INPOL ist auch jeder Verbundteilnehmer zur Eingabe und zum Abruf von Daten befugt. Bei Speicherungen in dem Verbundsystem INPOL kann das Bundesland, welches die personenbezogenen Daten eingegeben hat, diese beauskunften und auch löschen. Häufig weiß die betroffene Person nicht, welches Bundesland für die Datenerhebung und Speicherung in INPOL verantwortlich ist. Um es zu vermeiden, dass Bürgerinnen und Bürger 16 Anfragen auf Auskunft und gegebenenfalls Löschung stellen müssen, gibt auch das Bundeskriminalamt selbst Auskunft und nimmt gegebenenfalls auch die Löschung in INPOL vor.

5.5 Polizeilicher Umgang mit psychisch Auffälligen

Eine Dienstanweisung regelt den Umgang der Polizei mit psychisch auffälligen Personen im Rahmen der Gefahrenabwehr. Dabei kann es sowohl um Fälle der Eigengefährdung der psychisch auffälligen Personen selbst als auch um Fälle von Fremdgefährdungen durch diese psychisch auffälligen Personen gehen. Eine ärztliche Feststellung, dass die in Rede stehende Person psychisch krank ist, liegt dann (noch) nicht vor. In bestimmten Fällen dieser Art informiert die Polizei die zuständigen öffentlichen Stellen über eine mögliche psychische Erkrankung per Fax.

Uns erreichte eine Beschwerde über das Vorgehen der Polizei im Hinblick darauf, dass eine Datenübermittlung von der Polizei an das für die betreffende Person zuständige Behandlungszentrum erfolgte, der ein Beratungsgespräch des Behand-

lungszentrums angeboten worden war. Im Rahmen unserer datenschutzrechtlichen Kontrolle stellte sich heraus, dass gemäß dieser oben genannten Dienstanweisung auch eine Datenübermittlung an das für die Unterbringung nach dem Gesetz über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten zuständige Stadtamt sowie an das Landeskriminalamt Bremen stattgefunden hatte, obwohl im vorliegenden Fall keine Gefährdungslage gegeben war, und die Polizei außerhalb ihrer Befugnisse nach dem Bremischen Polizeigesetz handelte. Die Datenübermittlungen der Polizei an die jeweiligen Behörden waren daher datenschutzrechtswidrig, weil sie sich nicht auf die Datenübermittlungsbefugnis innerhalb der Polizei stützen konnte.

Die Polizei sagte zu, künftig lediglich den betroffenen Personen zu empfehlen, psychische Hilfen in Anspruch zu nehmen. Von einer Benachrichtigung der oben genannten Stellen wird künftig bei einer reinen psychischen Auffälligkeit ohne Gefährdungspotenzial abgesehen. Aus diesem Anlass haben wir uns vorgenommen, die oben genannte Dienstanweisung zu überprüfen.

5.6 Verwendung des personenbezogenen Hinweises „psychisch auffällig“ durch die Polizei Bremen bei Altfällen

Personenbezogene Hinweise (PHW) dienen in erster Linie der Eigensicherung der Polizei und werden im Rahmen der Einsatztaktik berücksichtigt. Der PHW „psychisch auffällig“ wurde bundesweit nur im Land Bremen nach der Dienstanweisung über polizeiliche Maßnahmen gegenüber psychisch auffälligen Personen aus dem Jahr 2003 auch dann vergeben, wenn keine psychische Krankheit durch einen Arzt festgestellt worden war. Nachdem wir auf die Gefahr einer Stigmatisierung der Betroffenen sowie auf die Schwierigkeiten, den Hinweis korrigieren oder löschen zu lassen, hingewiesen hatten, wurde uns vom Senator für Inneres und Sport zugesagt, den PHW „psychisch auffällig“ nicht mehr zu vergeben. Es werde nur noch das Merkmal „psychisch krank“ verwendet, das der Feststellung einer psychischen Erkrankung durch einen Facharzt bedarf. Ungeklärt war noch der Umgang mit den sogenannten Altfällen, in denen das PHW „psychisch auffällig“ bereits gespeichert war (vergleiche 32. Jahresbericht, Ziffer 5.3). In der Zwischenzeit ist uns vom Ressort mitgeteilt worden, dass auf Grundlage der neuen Erfassungskriterien eine Datenbereinigung in den noch vorhandenen Fällen stattgefunden habe und unserer Aufforderung zur Löschung von unzulässigen Speicherungen nachgekommen wurde.

5.7 Übergreifende Datenschutzkonzepte bei der Polizei Bremen

In diesem Berichtsjahr hat die Polizei Bremen uns den Entwurf eines Rahmendatenschutzkonzepts vorgelegt. Bei unserer Stellungnahme fiel uns ein wesentlicher Punkt auf, nämlich, dass das Rahmendatenschutzkonzept Verweise auf Soll-Vorschriften der Polizei Bremen enthält. Diese Soll-Angaben geben grundsätzlich keinen Ist-Zustand wieder, der aber für die datenschutzrechtliche und datenschutztechnische Bewertung maßgeblich ist und daher in einem Datenschutzkonzept beschrieben werden muss. Dieser unverbindliche Charakter des Rahmendatenschutzkonzepts steht im Gegensatz zu den verbindlichen Anforderungen an die Dokumentationspflicht der technischen und organisatorischen Maßnahmen gemäß § 7 Absatz 2 Satz 2 des Bremischen Datenschutzgesetzes (BremDSG) und zur Verbindlichkeit der technischen und organisatorischen Maßnahmen gemäß § 7 Absatz 3 und Absatz 4 Satz 2 des BremDSG und stellt damit den Sinn und Zweck der technischen und organisatorischen Maßnahmen (technischer und organisatorischer Schutz der personenbezogenen Daten) infrage.

Aktualisierungsbedarf gibt es derzeit auch bei den technischen Konzepten, die dem Rahmendatenschutzkonzept als Anlagen beigefügt sind. Weiterhin haben wir zum Benutzer- und Berechtigungskonzept der Polizei Bremen Stellung genommen. Insbesondere sehen wir hier Ergänzungsbedarf im Bereich der Administration sowie bei der Beschreibung der Prozesse zur Zugangskontrolle mit Chipkarte. Wir gehen davon aus, dass unsere Hinweise zwischenzeitlich Eingang in die Weiterentwicklung der Konzepte gefunden haben.

5.8 Stopp der Jugendgewalt

Bereits im 32. Jahresbericht hatten wir unter Ziffer 5.2 über das Projekt „Stopp der Jugendgewalt“ berichtet. Das Vorhaben, das aus einer Reihe von einzelnen Maßnahmen besteht, wurde vor dem Hintergrund einer zunehmenden Anzahl von durch

Jugendliche und Heranwachsende begangenen Gewaltdelikten ins Leben gerufen. Es bezweckt, jugendliche Täterinnen und Täter, die bereits einige Male in Erscheinung getreten sind, von einer kriminellen Karriere abzuhalten.

Personenorientierte Berichte

Personenorientierte Berichte enthalten eine Zusammenfassung seitens der Staatsanwaltschaft und der Polizei gesammelten Erkenntnisse über jugendliche oder heranwachsende Intensivtäterinnen oder Intensivtäter, um dadurch einen umfassenden Gesamtlebenslauf zu erhalten. Dadurch sollen wirkungsvolle Interventionen eingeleitet werden können. Die Bedenken, die wir hinsichtlich dieser Maßnahme hatten, konnten weitestgehend ausgeräumt werden. Es liegt uns allerdings nach wie vor noch kein Datenschutzkonzept zur geplanten Nutzung eines elektronischen Aktenverwaltungssystems vor.

Derzeit werden die personenorientierten Berichte auf Betriebssysteme durch das zuständige Kommissariat bearbeitet. Dadurch ist die Eingabekontrolle nach § 7 Bremisches Datenschutzgesetz (BremDSG) technisch nicht gegeben, da eine Protokollierung nur manuell auf dem entsprechenden Formblatt angelegt wird. Es handelt sich hier um eine organisatorische Lösung, die nicht revisionsfähig ist. Sie kann daher aus unserer Sicht nur eine Übergangslösung sein und sollte kurzfristig abgelöst werden. Eine Verfahrensbeschreibung zur Erstellung der personenorientierten Berichte wird nach Auskunft des Senators für Inneres und Sport derzeit von der Polizei Bremen erarbeitet. Zu dieser werden wir dann noch einmal gesondert Stellung nehmen.

Behördenübergreifende Fallkonferenzen

Behördenübergreifende Fallkonferenzen sollen im Sinne einer Ultima Ratio als Instrument zur Verstärkung staatlichen Handelns eingesetzt werden. Durch eine gemeinsame Analyse und Bewertung des Sachverhalts und der bisherigen Maßnahmen soll einerseits festgestellt werden, weshalb die bisherigen Hilfen und Interventionen nicht erfolgreich waren, und andererseits nach abgestimmten Lösungen gesucht werden. Wir haben hinsichtlich der Durchführung der Fallkonferenzen erhebliche datenschutzrechtliche Bedenken geäußert und diese auszugsweise im 32. Jahresbericht unter Ziffer 5.2 dargestellt. Wir erhielten aus dem Haus des Senators für Justiz und Verfassung Gelegenheit zur Stellungnahme zur Formulierung eines Musters für eine Einwilligungserklärung. Von dieser Möglichkeit haben wir Gebrauch gemacht trotz unserer grundsätzlich ablehnenden Haltung zu Einwilligungserklärungen in Fällen, in denen gesetzliche Datenübermittlungsbefugnisse aufgrund bewusster Entscheidungen des Gesetzgebers fehlen. Nach Auffassung der beteiligten Senatsressorts soll die Übermittlung von Informationen über die Betroffenen demgegenüber auf deren Einwilligung gestützt werden. Problematisch ist zudem, dass der Kreis der teilnehmenden Stellen in der Einwilligungserklärung nicht konkret benannt wird. Neben Vertreterinnen und Vertretern der Polizei Bremen, des Amtes für Soziale Dienste beziehungsweise des Jugendamts sowie der zuständigen Schule können danach auch die Staatsanwaltschaft und die Ausländerbehörde an den Fallkonferenzen teilnehmen. Wir halten eine konkrete Aussage über die tatsächliche Teilnahme der Staatsanwaltschaft und des Ausländeramts an der geplanten Fallkonferenz für erforderlich. Nur so kann dem Betroffenen die Tragweite seiner Einwilligung bewusst und eine informierte Erklärung abgegeben werden. Vom Senator für Inneres und Sport wurde uns mitgeteilt, dass die beteiligten Ressorts unsere Bedenken nicht teilen. Dementsprechend wird an der Einwilligungslösung sowie an der unkonkreten Formulierung in der Einwilligung bezüglich des Teilnehmerkreises festgehalten.

Intensivtäterkonzept

Als Intensivtäterinnen und Intensivtäter werden in Bremen Personen definiert, die durch die gewohnheits- oder gewerbsmäßige Begehung von Straftaten mit Schwerpunkten in den Bereichen Eigentums- und Gewaltkriminalität aufgefallen sind und bei denen angenommen werden kann, dass sie weitere Straftaten begehen werden. Zunächst war die Erstellung einer Intensivtäter-Ranking-Liste und einer Intensivtäterdatei vorgesehen. Im 32. Jahresbericht unter Ziffer 5.2 hatten wir darauf hingewiesen, dass sowohl für die Intensivtäterliste als auch die Intensivtäterdatei eine Verfahrensbeschreibung und ein Datenschutzkonzept notwendig sind. Die Polizei Bremen teilte uns zwischenzeitlich mit, dass eine Umsetzung der Intensivtäterdatei nicht stattfinde. Eine aktuelle Verfahrensbeschreibung und Handlungs-

anleitung zur Intensivtäterliste wurden uns vorgelegt. Dazu haben wir eine Stellungnahme abgegeben. Nach Angaben der Polizei wurden die Datenschutzkonzepte erneut überarbeitet und liegen derzeit dem behördlichen Datenschutzbeauftragten zur Vorabkontrolle vor.

Schwellentäterkonzept

Das Schwellentäterkonzept wendet sich an straffällig gewordene Jugendliche und Heranwachsende, die als Mehrfachtäterinnen und Mehrfachtäter aufgefallen sind und bei denen sich abzeichnet, dass sie auch weiterhin Straftaten begehen werden, sie sich also am Anfang einer kriminellen Laufbahn befinden. Ziel des Konzepts ist die Reduzierung der Straftaten, insbesondere der Gewalttaten. Die Kooperationsvereinbarung zur Umsetzung des Projekts wurde von uns geprüft. Unsere Anmerkungen wurden teilweise umgesetzt.

Interventionsteams

Interventionsteams sollen unter ressortübergreifender Abstimmung auf Gewaltphänomene in Schulen und sonstigen öffentlichen Räumen zeitnah reagieren und Gefährdungslagen unmittelbar beseitigen. Dazu werden Fachteams gebildet, die eine fallübergreifende Situationsanalyse und -bewertung durchführen und anlassbezogen sowie situativ und zeitlich begrenzt tätig werden. In einem Gesprächstermin mit Vertreterinnen und Vertretern der Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales äußerten wir inhaltliche Bedenken gegen das Konzept. Wir wiesen darauf hin, dass wir konkrete Informationen zur abschließenden datenschutzrechtlichen Bewertung benötigen. In der Mitteilung des Senats zum 32. Jahresbericht, Ziffer 5.2, wird angemerkt, dass das Konzept überarbeitet worden sei und sich derzeit in der ressortübergreifenden Abstimmung befinde.

5.9 Datenschutzkonzepte beim Stadtamt Bremen

Beim Stadtamt stehen diverse Stellungnahmen und Anpassungen der Datenschutzkonzepte aus. Exemplarisch haben wir folgende Datenverarbeitungsverfahren herausgesucht.

Zum AusländerDatenVerwaltungs- und InformationsSystem (ADVIS) haben wir bereits im Jahr 2007 Stellung genommen. Aufgrund personeller Engpässe im Stadtamt kam es zu zeitlichen Verzögerungen, sodass hier eine Beantwortung unserer Stellungnahme immer noch aussteht. Aus diesem Anlass möchten wir die von uns genannten Datenschutzaspekte an dieser Stelle artikulieren. Abgesehen von der Verpflichtung zur Nennung der speziellen Rechtsgrundlagen haben wir datenschutzrechtlich unter anderem auf die gesetzliche Verpflichtung aufmerksam gemacht, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungsgebot). Des Weiteren haben wir zum Beispiel darauf hingewiesen, dass die Religionszugehörigkeit der Ausländerinnen und Ausländer ein besonders schützenswertes personenbezogenes Datum darstellt und nach der Aufenthaltsverordnung und dem Gesetz über das Ausländerzentralregister nur auf freiwilliger Basis erhoben werden darf. Aus technischer Sicht besteht unter anderem Ergänzungsbedarf zur Weitergabekontrolle in Bezug auf Standortanbindungen und Filetransfers (Datenübertagungen), zum Berechtigungskonzept sowie zur Protokollierung.

Das Datenschutzkonzept Mobiler BürgerService wurde uns in diesem Jahr übersandt. Das Stadtamt setzt keine mobilen Endgeräte ein, sodass die datenschutzrechtlichen Aspekte begrenzt sind. Der Datenschutz stellt aufgrund der Nutzung der Räumlichkeiten durch unterschiedliche Stellen an den Zugriffsschutz (der Personalcomputer) erhöhte Anforderungen. Es ist zu gewährleisten, dass die zur Benutzung 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). Insbesondere ist dies im Hinblick auf die anderen Nutzerinnen und Nutzer der Räumlichkeiten, wie zum Beispiel der Deutschen Rentenversicherung Bund und der BürgerOnlineRedaktion im Stadtteil Osterholz (BORiS), sicherzustellen. Die hierzu eingereichten Unterlagen befinden sich derzeit in der Prüfung.

Das Stadtamt bedient sich des Hess Zahlungssystems zur Aufgabenerfüllung. Unsere Stellungnahme aus dem Jahr 2007 beschäftigte sich datenschutzrechtlich mit den Aspekten der Zutrittskontrolle, der Weitergabekontrolle und der Auftragsdaten-

verarbeitung. Aufgrund personeller Engpässe im Stadtamt kam es zu zeitlichen Verzögerungen, sodass hier eine Auskunft des Stadtamts noch aussteht. Das Stadtamt teilte uns mit, dass zwischenzeitlich umfangreiche Verfahrensänderungen vorgenommen worden sind, sodass wir von einer vollständigen Überarbeitung des Datenschutzkonzepts ausgehen.

Im IT-Fachverfahren IKONIZER zur Verwaltung der Schließanlage steht noch die Beantwortung unserer Datenschutzgesichtspunkte Zugangs-, Zugriffs-, Weitergabe- und Eingabekontrolle aus, die wir im Jahr 2007 dem Stadtamt mitgeteilt haben.

Seit geraumer Zeit haben wir keine adäquate Ansprechperson für das Datenverarbeitungsverfahren FundInfo, in dem es um die Verwaltung von Fundsachen geht. Wir bitten seit 2006 um nähere Auskunft über den Stand des Datenschutzkonzepts und der Verfahrensbeschreibung, insbesondere zu der Dienstanweisung und weiteren Maßnahmen zur Zugriffskontrolle. Die geplante und angekündigte Nutzung des Systems FundInfo durch die Polizei Bremen (siehe 29. Jahresbericht, Ziffer 9.21) findet nach Auskunft des Stadtamts und der Polizei Bremen derzeit nicht statt. Sollte die Nutzung des Systems ausgeweitet werden, sind auch hierfür konkrete Konzepte zu erstellen.

Betreffend das Datenschutzkonzept über die automatisierte Datenverarbeitung in der Waffenverwaltung (Waffenregister) fehlen uns noch ergänzende Auskünfte zu den Datenschutzthemen Anmeldeverfahren, Berechtigungskonzept und Eingabekontrolle. Vor dem Hintergrund der Einführung eines deutschen Waffenregisters mit der Schnittstelle XWaffe baten wir das Stadtamt um Informationen, welche Auswirkungen diese Neuerung auf das Bremische Waffenregister habe, insbesondere in Anbetracht der Integration von Echtdaten (siehe Ziffer 5.16 dieses Berichts).

Das allgemeine Rahmendatenschutzkonzept sowie das IT-Betriebskonzept wurden von uns umfassend geprüft. Nach Auskunft des Stadtamts findet derzeit eine Aufarbeitung unserer Stellungnahmen zu den Konzepten statt.

5.10 Abhandenkommen eines polizeilichen Führungszeugnisses beim Stadtamt

Ein Petent teilte uns mit, dass er beim Stadtamt ein polizeiliches Führungszeugnis beantragt habe, welches er für die Ausstellung einer Reisegewerbekarte benötige. Da die Bearbeitung der Reisegewerbekarte sehr lange dauerte, habe er sich beim Stadtamt nach dem Grund erkundigt. Von dort aus sei ihm mitgeteilt worden, dass sein Führungszeugnis verloren gegangen sei und erst ein neues beantragt werden musste. Der Petent wollte wissen, wo sich sein abhanden gekommenes Führungszeugnis nun befinde. Auf unsere Nachfrage hin wurde uns mitgeteilt, dass aufgrund des gegenüber dem Bundeszentral- und Gewerberegister angegebenen Verwendungszwecks das Führungszeugnis dem falschen Fachbereich im Stadtamt zugeordnet und dort verwahrt worden sei. Eine dortige Nachfrage des federführenden Fachbereichs unterblieb, sodass irrtümlich der Verlust des Führungszeugnisses angenommen wurde. Unberechtigte konnten nach Angaben der Behörde keine Kenntnis erhalten. Das Stadtamt wies nach eigenen Angaben seine ServiceCenter noch einmal ausdrücklich darauf hin, bei der Beantragung von Führungszeugnissen auf die richtige Angabe des Verwendungszwecks hinzuwirken. Zudem seien die Fachbereiche mit sich überschneidenden Aufgaben angehalten worden, sich besser abzustimmen und gegebenenfalls untereinander die erforderlichen Nachfragen zu halten.

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

Bereits im 31. Jahresbericht, Ziffer 9.3 und im 32. Jahresbericht, Ziffer 5.12, berichteten wir über unsere Forderung gegenüber dem Senator für Inneres und Sport, automatisierte Direktzugriffe von Gemeindebehörden auf die Melderegisterdaten der jeweiligen kommunalen Meldebehörden in Bremen beziehungsweise in Bremerhaven nur aufgrund einer gesetzlichen Grundlage zu gestatten. Diese Anforderung ergibt sich aus dem Bremischen Meldegesetz. Anlass, Zweck, Datenübermittlungsumfang und empfangende Stelle müssen dabei klar bestimmt sein, nicht zuletzt deshalb, damit die Datenübermittlungen für Bürgerinnen und Bürger jederzeit nachvollziehbar sind. Nach einem Auslegungserlass des Senators für Inne-

res und Sport an die nachgeordneten Meldebehörden kann eine Weitergabe der Meldedaten von der Meldebehörde in Bremen an sonstige öffentliche Stellen der Stadtgemeinde Bremen jedoch auch ohne eine spezielle gesetzliche Regelung der Datenübermittlung erfolgen. Begründet wurde diese Auffassung mit einer vermeintlich spezielleren Regelung im Bremischen Meldegesetz. Unter ausführlicher Darlegung unserer Rechtsauffassung hatten wir dem Senator für Inneres und Sport mitgeteilt, dass wir den Erlass als rechtswidrig erachten und um dessen Aufhebung gebeten. Auf Nachfrage wurde uns vom Senator für Inneres und Sport mitgeteilt, dass der Erlass nicht außer Kraft gesetzt worden sei. Bisher seien drei kommunale Behörden für den automatisierten Direktzugriff frei geschaltet worden, wovon jedoch nur zwei Behörden, namentlich die Einbürgerungsbehörde und das Amt für Wohnungswesen, den Zugriff nutzten. In der Stellungnahme des Senats zum 32. Jahresbericht der Landesbeauftragten für Datenschutz (Mitteilung des Senats vom 24. August 2010) wurde eine Novellierung der Meldedatenübermittlungsverordnung in Aussicht gestellt, in deren Rahmen das Thema geklärt werden solle. Wir gehen davon aus, dass unsere Bedenken dabei Berücksichtigung finden werden.

5.12 Zensus 2011

Aufgrund von Vorgaben der Europäischen Union (EU) sind alle Mitgliedstaaten im Jahr 2011 verpflichtet, eine Volks- und Wohnungszählung durchzuführen. Den Mitgliedstaaten bleibt dabei ein Spielraum, in welcher Form sie den Zensus vornehmen. In Deutschland hat man sich für eine Methode entschieden, die neben der Auswertung mehrerer Datenquellen auch eine Verknüpfung von Vollerhebungen mit Stichproben umfasst. Das bedeutet, dass die meisten Informationen aus den bereits vorhandenen Melderegistern, Datenbeständen der Bundesagentur für Arbeit sowie Dateien zum Personalbestand der öffentlichen Hand gewonnen und Haushalte nur stichprobenhaft befragt werden. Ziel des Zensus ist zum einen die Feststellung der amtlichen Einwohnerzahl Deutschlands, zum anderen, Informationen zum Wohnraum, zur Bildung und zum Erwerbsleben der Bevölkerung zu gewinnen. Das Zusammenfügen einer derart großen Anzahl von personenbezogenen Daten schafft naturgemäß besondere datenschutzrechtliche Risiken. Vor diesem Hintergrund hatten Bürgerrechtlerinnen und Bürgerrechtler eine Verfassungsbeschwerde gegen den Zensus 2011 vor dem Bundesverfassungsgericht eingelegt, der sich online mehr als 13 000 Menschen anschlossen. Kritisiert wurde insbesondere, dass die Zensusdaten über eine eindeutige Personenkennziffer vier Jahre lang zuzuordnen seien. Bemängelt wurde zudem, dass nach der Religionszugehörigkeit gefragt werde, obwohl die EU-Vorgabe dies nicht vorschreibe. Die Verfassungsbeschwerde wurde vom Bundesverfassungsgericht nicht zur Entscheidung angenommen, da die Beschwerdeschrift nicht die Mindestanforderungen an die Begründung von Verfassungsbeschwerden erfülle. Diese auf formale Gründe gestützte zurückweisende Entscheidung ändert nichts daran, dass an die Durchführung des Zensus 2011 strenge datenschutzrechtliche Anforderungen zu stellen sind und deren Einhaltung genauestens zu überprüfen ist.

Gesetzliche Grundlagen für den Zensus 2011 befinden sich im Zensusgesetz 2011, im Zensusvorbereitungsgesetz 2011, in der europäischen Verordnung über Volks- und Wohnungszählungen, in der Stichprobenverordnung, dem Bundesstatistikgesetz sowie in den Ausführungsgesetzen der Länder. Zum Entwurf des Bremischen Gesetzes zur Ausführung des Zensusgesetzes 2011 haben wir ausführlich Stellung genommen. Ein Großteil unserer Anmerkungen wurde dabei berücksichtigt. Nicht berücksichtigt wurden beispielsweise unsere Anregung, den Begriff „Erhebungsunterlagen“ in der Gesetzesbegründung zu präzisieren sowie unsere Forderung, in der Gesetzesbegründung einen Passus zu ändern, der besagt, dass Mitarbeiterinnen und Mitarbeiter aus sensiblen Bereichen des Verwaltungsvollzugs in den örtlichen Erhebungsstellen nicht eingesetzt werden, „vorausgesetzt, die personelle Ausstattung der kommunalen Körperschaft lässt dies zu“. Nach unserer Auffassung muss sichergestellt werden, dass entsprechende Mitarbeiterinnen und Mitarbeiter unter keinen Umständen in den Erhebungsstellen eingesetzt werden. Daher sollte der einschränkende Halbsatz in der Gesetzesbegründung gestrichen werden. Zudem halten wir es grundsätzlich für problematisch, dass für die Verfolgung von Ordnungswidrigkeiten nach dem Bremischen Zensusausführungsgesetz in Bremerhaven der Magistrat zuständig ist, denn dadurch besteht die Möglichkeit, dass Statistikdaten den besonders geschützten Bereich des Statistischen Landesamts verlassen. Das Gesetz trat im Herbst des Berichtjahres in Kraft.

Zudem haben wir das Datenschutzkonzept des Statistischen Landesamts zum Zensus 2011 geprüft und gehen davon aus, dass noch offene Punkte in Kürze geklärt werden. Um uns ein genaues Bild von der Sicherheit der Zensusdaten im Statistischen Landesamt zu machen, haben wir die Räumlichkeiten vor Ort besichtigt und Hinweise gegeben, sofern Verbesserungsbedarf bestand. Datenschutzrechtliche Bedenken geäußert haben wir hinsichtlich der in Bremen geplanten Beauftragung eines externen Dienstleisters mit dem Druck, der Personalisierung, der Kuvertierung und dem Versand sowie der Rücklaufkontrolle der Fragebögen. Dadurch bekommt der private Dienstleister ein komplettes Eigentümerverzeichnis in die Hände.

Ein enger Austausch zu den Datenschutzproblemen des Zensus 2011 findet mit den Datenschutzbeauftragten des Bundes und der anderen Länder im Rahmen des Arbeitskreises Statistik und der Ad-hoc-Arbeitsgruppe zum Zensus 2011 statt.

5.13 Neuer elektronischer Personalausweis

Seit dem 1. November 2010 können Bürgerinnen und Bürger den neuen elektronischen Personalausweis beantragen. Im Gegensatz zum bisherigen Personalausweis enthält der neue Ausweis einen Computer-Chip im Inneren der Karte, auf dem unter anderem ein digitales Foto und, auf freiwilliger Basis, zwei digitale Fingerabdrücke gespeichert werden. Der Chip soll zudem den elektronischen Identitätsnachweis ermöglichen, der für Anwendungen im Bereich E-Government und Authentisierung im Bereich E-Commerce genutzt werden kann. Eine Speicherung der Fingerabdrücke auf dem Personalausweis sollte sorgfältig abgewogen werden, da ein Missbrauchsrisiko, auch wenn Biometriedaten besonders geschützt sind, nicht völlig auszuschließen ist. Auch das Ausweisen gegenüber Behörden oder Privaten über das Internet birgt Risiken. So kann die Ausweis-PIN (Persönliche Identifikationsnummer) beispielsweise durch Unberechtigte ausgelesen werden. Das kann passieren, wenn bestimmte Lesegeräte genutzt werden. Lesegeräte ohne eigene Zifferntastatur erfordern es, dass die PIN über die normale Tastatur des PC eingegeben wird. Und dabei können die Tastatureingaben mit speziellen Programmen, die alle Tastatureingaben registrieren und aufzeichnen, mitgelesen werden. Diese Programme werden Keylogger genannt und sind frei im Internet verfügbar. Die Keylogger-Funktionalität ist oft integraler Bestandteil von Schadsoftware, wie sogenannte Trojaner dies beispielsweise sind.

Die Umsetzung der datenschutzrechtlichen Anforderungen beim Stadtamt werden von uns geprüft.

5.14 Datenschutz in Sportvereinen

Der Datenschutz erreicht immer mehr die Sportvereine. Mitglieder von Sportvereinen treten mit unterschiedlichen Fragen an uns heran. Ein Beispiel dafür ist die datenschutzrechtlich relevante Frage, ob die Übersendung von Mitgliederlisten an die Vorstandsmitglieder via E-Mail zulässig ist. Grundsätzlich kommt es hinsichtlich der Zusendung von Mitgliederlisten an die Vorstandsmitglieder darauf an, für welchen Vereinszweck das jeweilige Vorstandsmitglied welche Mitgliederdaten benötigt. An Vorstandspersonen, die für die Vorstands- und damit Vereinsarbeit Mitgliedernamen benötigen, darf grundsätzlich eine Mitgliederliste mit Mitgliedsnamen übermittelt werden. Was über die Mitgliedsnamen hinaus den Vorstandsmitgliedern übermittelt wird, hängt von dem Zweck und damit von der Funktion des Vorstandsmitglieds ab. Danach wird differenziert, weshalb das jeweilige Vorstandsmitglied welche Mitgliederdaten benötigt. Folglich hängt der Inhalt der Mitgliederliste von der jeweiligen Vorstandstätigkeit ab. Anschließend wird beurteilt, welche weiteren Angaben über die Mitglieder den jeweiligen Vorstandspersonen zur Verfügung gestellt werden dürfen. Die Weitergabe der Mitgliederdaten ist ein vereinsinterner Vorgang und stellt eine Nutzung von Daten dar. Aus datenschutztechnischer Sicht ist eine Überlassung von Mitgliederdaten via E-Mail zur Wahrung der Vertraulichkeit auf dem Übertragungsweg nur per Verschlüsselung datenschutzrechtlich zulässig. Mit unverschlüsselten E-Mails sind daher grundsätzlich keine personenbezogenen Daten, wie zum Beispiel Mitgliederlisten, zu versenden. Sofern keine Verschlüsselungssoftware eingesetzt wird, empfehlen wir grundsätzlich die Übersendung von Mitgliederlisten auf dem Postweg, um sich datenschutzkonform zu verhalten. Die Vereinsmitglieder haben auch die Möglichkeit, ein Faltblatt zum Thema „Datenschutz im Verein“ bei uns anzufordern. Im Internet können sich Vereine über kostenlose Verschlüsselungssoftware informieren, beispielsweise über das Bundesamt für Sicherheit in der Informationstechnik.

5.15 Stellungnahme zu den Verfassungsbeschwerden gegen das Bundeskriminalamtgesetz

Derzeit sind beim Bundesverfassungsgericht in Karlsruhe Beschwerden gegen das Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG) anhängig. Grund für diese Verfassungsbeschwerden ist die Änderung dieses Gesetzes, die im Jahr 2009 in Kraft trat. Diese Änderung umfasste verschiedene Punkte: der Aufgabenbereich des Bundeskriminalamts wurde auf den internationalen Terrorismus ausgedehnt und es wurden neue Befugnisregelungen zur Gefahrenabwehr des internationalen Terrorismus geschaffen. Der umstrittenste Aspekt betrifft wohl die sogenannte Onlinedurchsuchung.

Das Bundesverfassungsgericht hat allen Landesdatenschutzbeauftragten die Gelegenheit zur Stellungnahme eröffnet. In der gemeinsamen Stellungnahme rügen wir die Unbestimmtheit und Unverhältnismäßigkeit von Befugnisnormen zur Nutzung besonderer Mittel der Datenerhebung und zum Einsatz technischer Mittel in und aus Wohnungen, die Unbestimmtheit des Begriffs Kontakt- und Begleitperson sowie die Verfassungswidrigkeit der Regelung zur Rasterfahndung.

Im Raum steht auch die Regelung zum verdeckten Eingriff in informationstechnische Systeme. Unter dieser „Onlinedurchsuchung“ wird die heimliche Infiltration eines informationstechnischen Systems durch den Staat verstanden, indem über das Internet alle Dateien eines Personalcomputers durchsucht werden. Betretensrechte der Wohnung sind nach unserer Auffassung von dieser Vorschrift nicht erfasst. Insbesondere sind die Anordnungsfrist und die „Sichtungsregelung“ unverhältnismäßig. Letztere beschreibt, wer die Unterlagen und damit die personenbezogenen Daten ansieht und entscheidet, ob diese Kernbereichsrelevanz für die private Lebensgestaltung haben und somit gelöscht werden müssen oder nicht. Derzeit sind dafür Mitarbeiterinnen und Mitarbeiter des Bundeskriminalamts zuständig. Wir fordern eine richterliche Zuständigkeit (sogenannter Richtervorbehalt) für die Beurteilung dieser grundrechtsrelevanten Frage.

Weiterhin haben wir Vorbehalte gegen die Überwachung der Telekommunikation, insbesondere gegen die Regelungen zur Quellen-Telekommunikationsüberwachung, die Regelung zur Erhebung von Telekommunikationsverkehrs- und Nutzungsdaten, die Regelung zur Datenübermittlung an ausländische Stellen, die Regelungen zur Benachrichtigung und zum Schutz zeugnisverweigerungsberechtigter Personen vorgetragen. Über die Verfassungsbeschwerden wurde bislang noch nicht entschieden.

5.16 Deutsches Waffenregister

In Bremen sind derzeit etwa 7 900 Waffenbesitzer und circa 20 000 Waffen registriert, in Bremerhaven sind es etwa 2 100 Waffenbesitzer und rund 4 300 Waffen. Bundesweit existieren 577 Waffenbehörden. Die Kontrollen betreffend den Waffenbesitz wurden seitens des Stadtamts Bremen und des Magistrats der Seestadt Bremerhaven verstärkt. Datenschutzrechtlich relevant in diesem Kontext ist das Deutschland-Online-Projekt über das nationale Waffenregister. Hintergrund ist die Umsetzungsnotwendigkeit der Europäischen Richtlinie über die Kontrolle des Erwerbs und des Besitzes von Waffen (91/477/Europäische Wirtschaftsgemeinschaft), die im Jahr 2008 geändert wurde (2008/51/Europäische Gemeinschaft), und eine Pflicht der Mitgliedstaaten regelt, „bis 31. Dezember 2014 ein computergestütztes zentral oder dezentral eingerichtetes Waffenregister“ einzuführen. Darauf hat Deutschland mit der Änderung des deutschen Waffengesetzes reagiert und in § 43 a Waffengesetz bestimmt, bis zum 31. Dezember 2012 ein nationales, elektronisch auswertbares Waffenregister zu errichten. Das nationale Waffenregister soll ein zentral von dem Bundesverwaltungsamt geführtes Register sein, welches die personenbezogenen Daten über eine Schnittstelle von den kommunalen Waffenbehörden erhält. Das bedeutet, dass die waffenrechtliche Sachbearbeitung, wie Datenerfassung und -berichtigung, bei den kommunalen Behörden verbleibt. Folgende Aspekte sind in diesem Zusammenhang von datenschutzrechtlicher Relevanz: Wie erfolgt die Integration der bereits bestehenden personenbezogenen Daten? Werden die Daten im örtlichen Waffenregister gelöscht, während sie im Zentralregister 20 Jahre lang historisiert werden? Und wann werden die personenbezogenen Daten durch wen wie gelöscht? Daneben werden polizeiliche Begehrlichkeiten durch ein solches Register geweckt. Die Polizei möchte einen (lesenden) Zugriff auf die-

se personenbezogenen Daten. Derzeit sind automatisierte, bundesweite, polizeiliche Auswertungen zum Gesamtbestand der Waffen und Erlaubnisse nicht möglich. Über eine Erweiterung des Datenbestands betreffend die Erlaubnisse nach dem Bundesjagdgesetz und nach dem Gesetz über explosionsgefährliche Stoffe wird bereits nachgedacht. Wir haben uns an das Stadtamt Bremen gewandt und um eine erste, allgemeine Auskunft zu diesem Thema gebeten.

5.17 Nachrichtendienstliches Informationssystem

Das nachrichtendienstliche Informationssystem wird in Bremen und bundesweit neu aufgestellt. Auch wird die Verbesserung der informationellen Zusammenarbeit von den Verfassungsschutzbehörden durch eine technische Vereinheitlichung angestrebt. Die neue Ausrichtung dieses Informationssystems der Verfassungsschutzbehörden schlägt sich in einer umfassenden Volltextverarbeitung mit Suchmöglichkeiten nieder. Nach jedem in einem elektronischen Dokument vorkommenden Wort oder Datum kann elektronisch gesucht werden, weil das Dokument als Ganzes erfasst wird. Dies bildet einen Paradigmenwechsel, der einen besonders intensiven Eingriff für das Grundrecht auf informationelle Selbstbestimmung bedeutet und im Widerspruch zu geltendem Recht steht (vergleiche Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3. und 4. November 2010, Keine Volltextsuche in Dateien der Sicherheitsbehörden, Ziffer 19.11 dieses Berichts). Da die Nachrichtendienste schon Informationen zu legalem Verhalten von Zielpersonen sammeln dürfen und in diesen Zusammenhängen auch Kontakte mit unverdächtigen Bürgerinnen und Bürgern zustande kommen, sind hier die datenschutzrechtlichen, von der Verfassung verbürgten Anforderungen besonders hoch. Daneben wird durch die Möglichkeit einer Volltextrecherche der Grundsatz der Zweckbindung ad absurdum geführt. Daher werden die Landesbeauftragten für den Datenschutz die Entwicklung des nachrichtendienstlichen Informationssystems genauestens beobachten und in Anbetracht der technischen Möglichkeiten beratend begleiten.

5.18 Bericht aus dem Arbeitskreis Sicherheit

Auch in diesem Jahr tagte wieder der Arbeitskreis Sicherheit der Datenschutzbeauftragten des Bundes und der Länder. Der Arbeitskreis dient dem Erfahrungs- und Informationsaustausch. Themen waren unter anderem:

— der Datenschutz in der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene,

— die Verfassungsbeschwerden gegen das Bundeskriminalamtgesetz (siehe Ziffer 5.15 dieses Berichts),

— die Bundeskriminalamt-Daten-Verordnung aus Juni 2010,

— die Behandlung von Auskunftsbegehren beim Verfassungsschutz,

— das Deutschland-Online-Projekt zum nationalen Waffenregister (siehe Ziffer 5.16 dieses Berichts),

— die Evaluierung des Terrorismusbekämpfungsgesetzes und

— polizeiliche Ermittlungen im Internet beziehungsweise in sozialen Netzwerken.

Bei dem letztgenannten Thema geht es darum, wie Ordnungswidrigkeitsverfahren und Strafverfahren mittels Internet aufgeklärt werden können. Insbesondere soziale Netzwerke eignen sich zur Informationsgewinnung für die Polizei. Dabei werden Accounts (Benutzerkonten) von der Polizei genutzt, die dem Nutzerkreis nicht offenbaren, dass es sich hierbei um die Polizei handelt. Vielmehr bestehen getarnte Accounts. Grund für die verdeckten Ermittlungen ist die Sperrung des Accounts der Polizei aufgrund der Allgemeinen Geschäftsbedingungen von privat betriebenen sozialen Netzwerken, die eine offene, polizeiliche Informationsgewinnung nicht erlauben. Die zivilrechtliche Schranke lässt die Polizei gegen sich nicht gelten, weil sie bei der Ermittlung von Straftaten hoheitlich handelt und daher ihrer Auffassung nach keinen Nutzungsvertrag eingeht. Nach Auffassung der Polizei sind die in sozialen Netzwerken offen gelegten, personenbezogenen Daten, wie zum Beispiel Fotos, öffentlich zugängliche Informationen. Die Polizei Bremen nutzt das Internet für Ermittlungen im Bereich der Sexualdelikte und des Menschenhandels ebenso wie für Fahndungszwecke bei Schwerstkriminalität. Aber auch zur Aufklärung von Vermisstenfällen bedient sie sich des Internet zur Informationsgewinnung im Bereich der Gefahrenabwehr. Über die Auslegung, was allgemein zugängliche Da-

ten sind, lässt sich hier genauso trefflich streiten wie über die Frage, ob eine konkrete, spezialgesetzliche Rechtsnorm im Bremischen Polizeigesetz erforderlich ist, da die Polizei Bremen ihr Handeln im Gefahrenabwehrrecht auf die Befugnisgeneralklausel stützt. Die parallele Problematik stellt sich im repressiven Bereich für die allgemeine Ermittlungsvorschrift der Strafprozessordnung, die nach Auffassung der Polizei den Zutritt zum sozialen Netzwerk erlaubt.

6. Justiz

6.1 Datenschutz bei der Zustellung durch Gerichtsvollzieherinnen und Gerichtsvollzieher

Im Berichtsjahr erhielten wir eine Beschwerde über eine im Land Bremen tätige Gerichtsvollzieherin. Unsere Petentin war Mitarbeiterin einer Gemeinschaftspraxis, welche zwar in einem Krankenhaus gelegen, aber keine Einrichtung des Klinikums war. Die Gerichtsvollzieherin sollte dem Arbeitgeber der Petentin einen Pfändungs- und Überweisungsbeschluss zustellen. Da die Praxis zum Zeitpunkt des Zustellungsversuchs nicht besetzt war, gab sie den Beschluss bei der Zentrale des Krankenhauses ab und verließ sich auf die Aussage der Mitarbeiterin der Zentrale, dass sie Zustellungen an die Arztpraxis immer entgegennehmen würde. Darüber hinaus übergab sie das zuzustellende Schriftstück ohne Umschlag und ließ es genügen, dass die Mitarbeiterin der Zentrale ihr versicherte, den Beschluss in einen Umschlag zu tun.

Die Übergabe eines nicht kuvertierten Pfändungs- und Überweisungsbeschlusses an eine nicht empfangsberechtigte Person stellt einen erheblichen datenschutzrechtlichen Verstoß dar. Bei dem Pfändungs- und Überweisungsbeschluss handelte es sich um einen Beschluss gegen die Petentin, welcher sensible Informationen über diese enthielt, die Dritten nicht hätten zugänglich gemacht werden dürfen. Lediglich der Arbeitgeber als Drittschuldner wäre berechtigt gewesen, die Daten zur Kenntnis zu nehmen.

Da die Angelegenheiten der Gerichtsvollzieherinnen und Gerichtsvollzieher der Dienstaufsicht des Präsidenten des Amtsgerichts unterliegen, haben wir diesen zur Stellungnahme aufgefordert. Dieser teilte unsere Einschätzung und wies die Gerichtsvollzieherin auf ihr Fehlverhalten hin unter Hinweis auf § 30 Nummer 2 und auf § 36 Nummer 3 der Geschäftsanweisung für Gerichtsvollzieher (GVGA).

Weiterhin teilte uns der Präsident des Amtsgerichts mit, dass die Gerichtsvollzieherin aufgefordert wurde, sich in Zukunft vorschriftsgemäß zu verhalten. Die übrigen Gerichtsvollzieherinnen und Gerichtsvollzieher des Amtsgerichtbezirks Bremen wurden ebenfalls für dieses Thema sensibilisiert.

6.2 Datenschutz beim Grundbuchamt

Eine Bürgerin beschwerte sich bei uns über die fehlende Diskretion beim Grundbuchamt. Mitte Mai 2010 hatte sie beim Grundbuchamt eine Akte eingesehen. Während der Akteneinsicht soll im gleichen Zimmer ein Sachbearbeiter gesessen und Telefongespräche geführt haben, sodass sie Informationen – auch über andere Bürger – habe mithören können. Außerdem sollen im Nebenzimmer Personen, die mit persönlichen Anliegen vorstellig wurden, bedient worden sein, sodass die Bürgerin deren Namen und andere private Informationen mitbekommen habe. Die Tür soll nicht geschlossen gewesen sein.

Auf unsere Nachfrage hin wurde die Situation beim Grundbuchamt erörtert und es wurden organisatorische Maßnahmen seitens der Behörde getroffen. Die Verbindungstür zwischen Rechtsantragsstelle und dem Einsichtsbereich wurde verschlossen, sodass keine persönlichen Daten der Rechtsantragsstelle mehr im Einsichtsbereich mitgehört werden können. Die Mitarbeiterinnen und Mitarbeiter im Einsichtsbereich wurden auf die Problematik des Datenschutzes bei Telefongesprächen in Anwesenheit von Publikum hingewiesen.

An diesem Beispiel zeigt sich, dass schon kleine organisatorische Maßnahmen und die Sensibilisierung von Beschäftigten zu einer Verbesserung des Datenschutzniveaus führen können.

6.3 Auskunftsersuchen von Bürgerinnen und Bürgern an die Staatsanwaltschaft

Zu unserer Tätigkeit gehört es, Auskunftsersuchen von Bürgerinnen und Bürgern gegenüber der Verwaltung zu unterstützen. Diese Auskunftsersuchen betreffen

auch bei der Staatsanwaltschaft gespeicherte personenbezogene Daten. Es herrscht diesbezüglich wohl ein Dissens zwischen der Staatsanwaltschaft und uns. Wenn wir den Bürgerinnen und Bürgern bei der Durchsetzung ihres Auskunftsanspruchs helfen, dann ist nicht das Auskunftsrecht gegenüber einer öffentlichen Stelle gemäß § 474 Strafprozessordnung einschlägig, sondern es bleibt bei dem Auskunftsrecht von natürlichen Personen, zum Beispiel gemäß § 491 Strafprozessordnung.

6.4 Prüfkompetenz der Landesdatenschutzbeauftragten bei der Staatsanwaltschaft

Bezüglich der Kontrollbefugnisse der Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) bei der Staatsanwaltschaft Bremen besteht Dissens, welcher immer wieder zu Problemen hinsichtlich der Ausübung der vom Gesetz vorgesehenen Datenschutzkontrolle führt.

Wir vertreten die Rechtsauffassung, dass sich unsere Prüfbefugnisse beziehungsweise Prüfverpflichtungen aus § 27 Absatz 1 Satz 1 Bremisches Datenschutzgesetz (BremDSG) ergeben. Hiernach überwacht die Landesbeauftragte für Datenschutz und Informationsfreiheit die Einhaltung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den in § 1 Absatz 2 BremDSG genannten Stellen. Die Staatsanwaltschaft Bremen ist eine Behörde im Sinne von § 1 Absatz 2 Satz 1 BremDSG und unterliegt damit der Kontrolle der Landesbeauftragten für Datenschutz und Informationsfreiheit, soweit datenschutzrechtlich relevante Verhaltensweisen, wie zum Beispiel die Datenerhebung, die Datenverarbeitung oder die Datenübermittlung, betroffen sind. Nach § 27 Absatz 1 Satz 1 BremDSG beschränkt sich die Zuständigkeit der Landesbeauftragten für Datenschutz und Informationsfreiheit nicht auf die Überwachung der Einhaltung der Vorschriften des Bremischen Datenschutzgesetzes, sondern umfasst auch die Kontrolle der Einhaltung anderer Vorschriften über den Datenschutz. Das bedeutet, dass die Landesbeauftragte für Datenschutz und Informationsfreiheit bei den in § 1 Absatz 2 BremDSG genannten Stellen auch die Einhaltung von bundesgesetzlichen datenschutzrechtlichen Regelungen überwacht, soweit diese von den Landesbehörden anzuwenden sind. Hierzu gehören neben der Strafprozessordnung eine Vielzahl von anderen Gesetzen, wie zum Beispiel das Sozialgesetzbuch und das Telemediengesetz. Beim Bremischen Datenschutzgesetz handelt es sich lediglich um ein Auffanggesetz, welches greift, wenn keine Spezialgesetze vorhanden sind oder diese keine abschließenden Regelungen enthalten. Die bundesrechtliche Regelung des Strafverfahrensrechts schließt eine landesrechtliche Regelung über die Verarbeitung personenbezogener Daten bei Landesbehörden nicht aus. Landesbehörden unterliegen damit den datenschutzspezifischen Regelungen des Landesrechts auch dann, wenn sie Bundesrecht ausführen. Des Weiteren sind auf die Landesbehörden, die Bundesrecht ausführen, gleichzeitig die datenschutzrechtlichen Bestimmungen des Landesrechts und zudem die bereichsspezifischen Datenschutzregelungen des Bundesrechts anwendbar. Damit unterliegt die Staatsanwaltschaft grundsätzlich der Überwachung der Landesbeauftragten für Datenschutz und Informationsfreiheit nach § 27 BremDSG.

6.5 Novellierung des Bremischen Datenschutzgesetzes aufgrund der Entscheidung des Europäischen Gerichtshofs zur Unabhängigkeit

In seinem Urteil vom 9. März 2010 hat der Europäische Gerichtshof (EuGH) festgestellt, dass die Bundesrepublik Deutschland gegen § 28 Absatz 1 Satz 2 der Datenschutzrichtlinie der Europäischen Gemeinschaft (EG) 95/46/EG verstößt. Nach dieser Regelung nehmen die Datenschutzkontrollstellen ihre Aufgaben in völliger Unabhängigkeit wahr. Dadurch, dass die für die Überwachung des Datenschutzes im nicht öffentlichen Bereich in den Bundesländern zuständigen Kontrollstellen der staatlichen Aufsicht unterstellt sind, fehle es an der völligen Unabhängigkeit.

In Bremen kontrolliert die Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) sowohl den öffentlichen als auch den nicht öffentlichen Bereich. Für den nicht öffentlichen Bereich gab es allerdings keine gesetzliche Regelung hinsichtlich der staatlichen Aufsicht, sodass die Europäische Kommission davon ausging, dass die Aufsichtsbehörde in Bremen sowohl der Fach- als auch der Dienstaufsicht unterlag (siehe 28. Jahresbericht, Ziffer 3.1).

Aufgrund der Entscheidung des Europäischen Gerichtshofs wurde das Bremische Datenschutzgesetz (BremDSG) novelliert. Es wurde klargestellt, dass die LfDI auch

bei der Ausübung ihrer Aufgaben im nicht öffentlichen Bereich keiner Fach- und Rechtsaufsicht unterliegt und nur dem Gesetz unterworfen ist. Zudem wurde festgestellt, dass die LfDI der Dienstaufsicht des Senats nur unterliegt, soweit ihre Unabhängigkeit nicht beeinträchtigt wird. Diese Regelungen gelten sowohl für den öffentlichen als auch für den nicht öffentlichen Bereich. Weiterhin wurde die alleinige Entscheidungsbefugnis der Landesbeauftragten über Aussagegenehmigungen und Aktenvorlagen bei Gericht geregelt und das Widerspruchsverfahren bei Anfechtungs- und Verpflichtungsklagen gegen die Landesbeauftragte für Datenschutz und Informationsfreiheit ausgeschlossen. Zudem vertritt die LfDI nunmehr die Freie Hansestadt Bremen im gerichtlichen Verfahren. Schließlich wurde eine maßgebliche Entscheidungsbefugnis der LfDI für die Stellenbesetzungen sowie maßgebliche personalrechtliche Entscheidungen normiert.

Im Zusammenhang mit der Novellierung des Bremischen Datenschutzgesetzes baten wir den Senator für Justiz und Verfassung auch für den Datenschutz im öffentlichen Bereich über Neuregelungen nachzudenken. Eine wichtige Änderung aus unserer Sicht wäre die Übertragung der Ordnungswidrigkeitsbefugnis vom Leitenden Oberstaatsanwalt auf die Landesbeauftragte für Datenschutz und Informationsfreiheit. Hierfür sprechen die Gesichtspunkte der Unabhängigkeit der Aufgabenwahrnehmung, der Sachnähe sowie der Vereinheitlichung von Entscheidungsmaßstäben. Zudem schlugen wir vor, einige im Bundesdatenschutzgesetz vorgesehene Regelungen zur Stärkung des Datenschutzes auch für den öffentlichen Bereich des Landes Bremen zu übernehmen. Hier sind insbesondere eine Konkretisierung der Auftragsdatenverarbeitung, die Anhebung der Obergrenze für Ordnungswidrigkeiten sowie eine Informationspflicht bei Datenschutzpannen zu nennen. Der Senator für Justiz und Verfassung erklärte sich bereit, über die Erhöhung des Bußgeldrahmens nachzudenken. Wir baten in einem weiteren Schreiben auch den anderen Punkten näherzutreten und hoffen, dass die Neuregelungen in Bezug auf den nicht öffentlichen Bereich nur ein erster Schritt gewesen sind und die datenschutzrechtlichen Regelungen auch für den öffentlichen Bereich im Land Bremen noch weiter verbessert werden.

7. Gesundheit und Soziales

7.1 Öffentlicher Bereich

7.1.1 Umstrukturierung der vier kommunalen Krankenhäuser durch Zentralisierung von Aufgaben

Seit mehreren Jahren unterliegen die vier kommunalen Krankenhäuser der Stadt Bremen einem intensiven Strukturwandel, der auch datenschutzrechtliche Auswirkungen hat. Erklärtes Ziel ist unter anderem, die gesamte Informationstechnologie der vier Kliniken auf die Gesundheit Nord gGmbH (GeNo) zu übertragen. Zu den zu zentralisierenden Servicebereichen sollen die Abrechung der Patientenbehandlung, Personal und Recht sowie Controlling gehören. Datenschutzrechtlich gesehen sind in diesem Prozess bei der Verarbeitung der Daten von Patientinnen und Patienten das Bremische Krankenhausdatenschutzgesetz (BremKHDSG) und bei der Verarbeitung von Beschäftigtendaten das Bremische Datenschutzgesetz (BremDSG) in Verbindung mit dem Bremischen Beamtengesetz einzuhalten.

Inzwischen hat die GeNo Klinikverbund Bremen Unterlagen vorgelegt, die eine Bewertung der Umstrukturierung ermöglichen. Wir haben der GeNo deutlich gemacht, dass auch aus datenschutzrechtlichen Gründen klar erkennbar sein muss, ob die GeNo oder die jeweilige Klinik für die einzelnen Aufgaben verantwortlich ist. Bei den so den einzelnen Organisationen zugeordneten Aufgaben ist im nächsten Schritt zu entscheiden, ob es sich um eine Funktionsübertragung oder eine Auftragsdatenverarbeitung handelt.

Funktionsübertragungen liegen vor, wenn Aufgaben der einzelnen Krankenhäuser auf die GeNo übertragen werden. Dies gilt hier zum Beispiel für Teilaufgaben der Personalverwaltung und sogenannte patientenferne Aufgaben, unter anderem das Labor und die Essensverpflegung. Neben einer Prüfung, ob die Zentralisierung patientenferner Aufgaben zur Durchführung des Behandlungsvertrags erforderlich ist, ist als Ergebnis der Vorabkontrolle festzulegen, dass insbesondere beim zentralisierten Labor und der zentralisierten Essensverpflegung von den Möglichkeiten der Pseudonymisierung Gebrauch zu machen ist.

Zur Wahrung der Rechte der Beschäftigten sowie der Patientinnen und Patienten hinsichtlich ihrer Auskunfts- und Akteneinsichtsrechte sind diese, gegebenenfalls in Form eines Merkblatts, darüber zu unterrichten, welche Daten zu welchen Zwecken beim Krankenhaus und welche bei der GeNo gespeichert und wo die Personalakten oder Patientenakten geführt werden.

Die Auftragsdatenverarbeitung liegt beispielsweise bei einer Beauftragung der GeNo ausschließlich zur automatisierten Verarbeitung der Beschäftigten- und Patientendaten durch die vier kommunalen Kliniken vor und die damit zu erfüllenden Aufgaben werden weiterhin vom Krankenhaus wahrgenommen. Hier bleiben die vier Kliniken auch datenschutzrechtlich verantwortlich für die Verarbeitung der personenbezogenen Daten; die GeNo ist lediglich Auftragnehmerin. Für die Auftragsdatenverarbeitung bedarf es vertraglicher Regelungen zwischen den vier Kliniken und der GeNo. Dabei sind insbesondere Umfang, Art und Zweck der vorgesehenen Datenverarbeitung, Art der Daten und Kreis der Betroffenen, Weisungsbefugnisse der vier Kliniken gegenüber der GeNo sowie technische und organisatorische Maßnahmen festzulegen.

Zum Schutz der Patientendaten und zur Einhaltung der besonderen Vorgaben des Bremischen Krankenhausdatenschutzgesetzes ist zudem ausdrücklich festzulegen, dass ein Zugriff auf Patientendaten durch die Auftragnehmerin, hier die GeNo, nur im Rahmen der Prüfung und Wartung von Datenverarbeitungsanlagen und automatisierten Verfahren erfolgen darf, wenn das jeweilige Krankenhaus im Einzelfall zuvor die Daten freigegeben hat. Das Gleiche gilt zur Sicherstellung dafür, dass die GeNo bei der Administration technischer Vorkehrungen zur Abwehr von Angriffen auf das Datenverarbeitungssystem so weit wie möglich keinen Zugriff auf Patientendaten nehmen kann.

Wir haben die GeNo Klinikverbund Bremen gebeten, uns eine Rahmenverfahrensbeschreibung sowie einen Rahmenvertrag zur Auftragsdatenverarbeitung zur Verfügung zu stellen und darauf hingewiesen, dass die übrigen genannten Anforderungen in Abstimmung mit den vier kommunalen Krankenhäusern zu beachten und umzusetzen sind. Dies ist inzwischen erfolgt.

7.1.2 Belegungsplan der Psychiatrie des Klinikums Bremen-Nord auf offener Straße

Ein Bürger hat uns den Belegungsplan der Psychiatrie des Klinikums Bremen-Nord gGmbH ausgehändigt mit dem Hinweis, ihn auf offener Straße gefunden zu haben. Auf dem Plan sind unter Nennung der vollständigen Namen und des Alters der Patientinnen und Patienten handschriftlich sehr sensible Angaben zu deren Erkrankung mit damit in Verbindung stehenden Vorkommnissen vermerkt.

Auf Anfrage hat uns das Klinikum Bremen-Nord gGmbH erklärt, das Dokument sei offensichtlich aus der Hosentasche eines Krankenpflegeschülers gefallen. Der Belegungsplan diene als Informationsstütze bei den Übergaben in der Psychiatrie. Grundsätzlich werde der Plan nur innerhalb der Psychiatrie gebraucht, was von dem Mitarbeiter nicht beachtet worden sei. Alle Beschäftigten der Psychiatrie seien angehalten, einen solchen Plan nach Ablauf der Dienstzeit in einem dafür vorgesehenen Schubladenfach zu deponieren.

Zum Schutz der höchst sensiblen Patientendaten auf dem Belegungsplan haben wir dem Klinikum dargelegt, dass die Anzahl der Kopien dieses Plans auf das unbedingt notwendige Maß zu beschränken ist und vorgeschlagen, nur noch ein Exemplar des Belegungsplans zu verwenden, der von den jeweils diensthabenden Beschäftigten in der Psychiatrie nur zum Zwecke der Übergabe eingesehen werden kann.

Daraufhin hat das Klinikum überzeugend entgegnet, dass ein entsprechender Belegungsplan allen einzelnen Beschäftigten im psychiatrischen Alltag zur Verfügung stehen müsse, weil es vor allem um schnelle Informationen bei Fragen der Ausgangsregelung oder sonstigen psychiatrischen Fragestellungen gehe. Unser Vorschlag würde eine seit Jahren bestehende, sehr gut funktionierende psychiatrische Praxis in äußerster Weise erschweren. Zudem sei mittlerweile ein Entsorgungsbehälter für datenschutzrelevante Fakten im Besprechungs- und Dienstzimmer aufgestellt worden. Außerdem seien alle Beschäftigten über die Problematik unterrichtet worden und wüssten, dass nach Dienstende die entsprechenden relevanten Daten dort hineingehörten.

7.1.3 Weitergabe eines Krankenhausentlassungsberichts an andere Ärzte als den Hausarzt

Ein Patient hat erklärt, nach seinem Aufenthalt in der Klinik für Neurologie im Klinikum Bremen-Ost gGmbH den Chefarzt gebeten zu haben, den Krankenhausentlassungsbericht nur an seinen Hausarzt zu übersenden. Stattdessen sei der Bericht auch an zwei Fachärzte des Patienten weitergegeben worden.

Auf Anfrage hat uns der Chefarzt der Klinik bestätigt, den Bericht auch an die beiden Fachärzte übersandt zu haben. Es sei nicht mehr nachvollziehbar, ob der Patient ausdrücklich verlangt habe, den Bericht nur an den Hausarzt zu übersenden. Grundsätzlich würden die Patienten zur Frage der Weitergabe von Arztbriefen befragt.

Daraufhin haben wir dem Chefarzt dargelegt, dass eine unzulässige Übermittlung personenbezogener Daten eine unzulässige Speicherung beim Datenempfänger zur Folge hat, die dazu führt, dass bei den Empfängern die Daten gelöscht werden müssen. Aus diesem Grund musste der Chefarzt die beiden Fachärzte auffordern, die ihnen unrechtmäßig zugesandten Krankenhausentlassungsberichte unverzüglich zu vernichten und uns dies zu bestätigen. Der Chefarzt hat uns daraufhin darüber unterrichtet, dass dies erfolgt sei.

7.1.4 Vertraulichkeit der Anmeldegespräche beim Ärztlichen Notdienst

Ein Bürger hatte seine Mutter im Taxi zum Ärztlichen Notdienst beim Klinikum Bremen-Mitte gGmbH begleitet. Er habe sie in einem Raum, der zum Flur nur mit einer Glasscheibe abgetrennt sei, angemeldet und um die Ausstellung eines Taxischeines gebeten. In dem Raum hinter der Glasscheibe hielten sich Personen auf, von denen er angenommen hatte, dass sie zum Personal gehörten. Nach Beendigung des Anmeldegesprächs sei eine Person davon auf den Petenten zugekommen, habe sich als Taxifahrerin ausgegeben und mit ihm über die Problematik der Ausstellung eines Taxischeins gesprochen. Kritisiert wird vom Petenten, dass dadurch zumindest dieser Person hinter der Glasscheibe des Anmelderaums die im Rahmen der Anmeldung erhobenen Gesundheitsdaten über seine Mutter zugänglich gemacht worden sind.

Die für den Ärztlichen Notdienst verantwortliche Kassenärztliche Vereinigung Bremen (KVHB) hat dazu erklärt, der Ärztliche Notdienst bediene sich eines Taxiunternehmens und deren Beschäftigte seien aufgrund eines Vertrages zur Verschwiegenheit verpflichtet.

Daraufhin haben wir der KVHB dargelegt, dass es trotz dieser Verschwiegenheitsverpflichtung nicht erforderlich ist, dass sich die Taxifahrerinnen und Taxifahrer in dem Raum hinter der Glasscheibe aufhalten und dadurch unbefugt Gesundheitsdaten zur Kenntnis nehmen. Aus diesem Grund haben wir von der KVHB verlangt, technische und organisatorische Maßnahmen zur Zutrittskontrolle zu treffen, die diese unbefugte Kenntnisnahme ausschließen.

Die KVHB hat daraufhin zugesagt, dass die Beschäftigten des Taxiunternehmens künftig keinen Zutritt mehr zu dem Raum der Annahmestelle haben.

7.1.5 Versendung eines amtsärztlichen Attests durch das Gesundheitsamt

Ein Student teilte uns mit, er habe für sich persönlich beim Gesundheitsamt ein amtsärztliches Attest beantragt. Nach Erstellung des Attests habe ihm das Gesundheitsamt mitgeteilt, das Attest sei an die Universität versandt worden. Die Universität habe ihm dazu mitgeteilt, sein dort anhängiges Verwaltungsverfahren sei aufgrund dieses Attests negativ beschieden worden.

Die Übersendung des Attests an die Universität steht im Widerspruch zur Rechtslage. Nach § 23 des Gesetzes über den öffentlichen Gesundheitsdienst (ÖGDG) erhält nur die Stelle das Attest, die die Untersuchung veranlasst hat.

Das Gesundheitsamt hat den Versand bestätigt und erklärt, die Abweichung vom ÖGDG habe sich aus einer Unklarheit ergeben. Es sei nicht klar gewesen, wer konkreter Auftraggeber des Attests sei. Zudem sei es zu einem anschließenden Versandfehler in der Geschäftsstelle gekommen. Im Übrigen habe das Amt nach diesem Vorfall veranlasst, dass in deren Datenbank die Auftraggeberin oder der Auftraggeber eindeutig benannt werde.

Wir haben die Behörde darauf hingewiesen, dass eine unzulässige Datenübermittlung eine unzulässige Datenspeicherung beim Datenempfänger zur Folge hat.

Aus diesem Grunde haben wir das Gesundheitsamt aufgefordert, bei der Universität auf die Vernichtung des Attests hinzuwirken. Dies ist uns inzwischen von der Universität bestätigt worden.

7.1.6 Datenübermittlung durch die Krankenkasse an das Jugendamt bei Verdacht auf Kindeswohlgefährdung

Die Allgemeine Ortskrankenkasse (AOK) Bremen/Bremerhaven hat uns ihre Auffassung mitgeteilt, wonach sich aus den Abrechnungsunterlagen der Ärztinnen und Ärzte sowie der Krankenhäuser häufig Hinweise auf einen Verdacht auf Kindeswohlgefährdung ergäben. Die Krankenkasse sei unsicher, wie in solchen Fällen zu verfahren ist. Sie wollte wissen, unter welchen Voraussetzungen sie Daten an das Jugendamt übermitteln dürfe.

Nach den Vorschriften des Fünften und Zehnten Sozialgesetzbuches besteht für die AOK keine Rechtsgrundlage zur Übermittlung derartiger Daten an das Jugendamt. Diese gesetzliche Wertung ist sachgerecht, weil die die Abrechnungsdaten erstellenden Kinderärztinnen und Kinderärzte durch Fortbildungen in der Beurteilung des Vorliegens von Anhaltspunkten für Kindeswohlgefährdungen geschult sind. Die unbefugte Übermittlung von Sozialdaten durch Sozialleistungsträger (die Krankenkassen) ist unter den Voraussetzungen des § 86 Zehntes Sozialgesetzbuch sogar eine Straftat.

Eine Übermittlung von Sozialdaten durch die Krankenkasse an das Jugendamt ist in einem rechtfertigenden Notstand unter den Voraussetzungen des § 34 Strafgesetzbuch zulässig. Danach handelt nicht rechtswidrig, wer in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben, Leib, Freiheit oder ein anderes Rechtsgut eine Tat begeht, um die Gefahr von einem anderen abzuwenden. Hierbei muss bei der Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigende wesentlich überwiegen. Dies gilt jedoch nur, soweit die Tat ein angemessenes Mittel ist, die Gefahr abzuwenden.

Wir haben der AOK vorgeschlagen, sich an die behandelnde Ärztin oder den behandelnden Arzt, aus deren oder dessen Abrechnungsunterlagen sich eventuelle Verdachtshinweise ergeben, zu wenden. Die Ärztin oder der Arzt hat dann zu entscheiden, ob ein Fall der Kindeswohlgefährdung vorliegt. In diesem Fall darf sie oder er unter den Voraussetzungen des § 34 Strafgesetzbuch das Jugendamt informieren. Dabei müssen die Eltern auf den Verdacht der Kindeswohlgefährdung hingewiesen und um eine Entbindung von der Schweigepflicht gegenüber dem Jugendamt gebeten werden. Wird diese verweigert, hat die Ärztin oder der Arzt die Eltern darauf hinzuweisen, dass sie oder er das Jugendamt einschalten wird. Wenn die Eltern dann noch immer die Einwilligung verweigern, wäre die Ärztin oder der Arzt zur Datenübermittlung an das Jugendamt befugt.

7.1.7 Warnung vor Verdacht auf Arzneimittelmissbrauch an alle Ärztinnen und Ärzte durch die Kassenärztliche Vereinigung

Die Kassenärztliche Vereinigung Bremen (KVHB) hat an alle niedergelassenen Vertragsärztinnen und Vertragsärzte im Land Bremen eine auf eine Patientin bezogene Warnung wegen vermuteten Arzneimittelmissbrauchs versandt. Dabei wurden Namen, Adresse, Geburtsdatum und Krankenkasse der Patientin genannt. Begründet wurde dies damit, dass die Patientin von einer Vielzahl von Ärztinnen und Ärzten eine hohe Anzahl von Arzneimitteln mit hohem Suchtpotenzial verschrieben bekommen habe. Die Patientin wurde über diese Warnmeldung nicht informiert. Wir haben die KVHB bei unserer Anfrage darüber unterrichtet, dass eine derartige Warnmeldung nicht zu ihren Befugnissen nach dem Fünften Sozialgesetzbuch gehört. Nach diesem Gesetz darf die KVHB personenbezogene Daten nur zur Abrechnungs- und Wirtschaftlichkeitsprüfung verarbeiten.

Die KVHB hat erklärt, die Betroffene lasse sich nach Angabe ihrer Krankenkasse seit Jahren das entsprechende Arzneimittel in einer hohen Menge verschreiben. Dies sei nicht mit einem medizinisch zu rechtfertigenden Eigenverbrauch zu erklären. Die Krankenkasse vermute eine sehr lebensbedrohende Eigengefährdung der Patientin. Ebenso sei eine Straftat nicht auszuschließen. Die Warnmeldung sei erforderlich gewesen, weil die KVHB und die Krankenkasse ein überragendes Interesse hätten, Arzneimittelmissbrauch oder sogar strafbaren Handlungen vorzubeugen beziehungsweise nachzugehen. Gerade weil jede Vertragsärztin und jeder Ver-

tragsarzt in ihrer oder seiner Entscheidung frei sei, entsprechende Arzneimittel zu verordnen, sei die Warnmeldung zur Eindämmung dieses Fehlverhaltens geeignet. Gleichwohl hat die KVHB vorgeschlagen, anstelle der bisherigen Daten lediglich die Versichertennummer der Patientin oder des Patienten in Warnmeldungen anzugeben.

Wir haben dazu entgegnet, dass der Vorschlag, lediglich die Versichertennummern verdächtiger Personen an die Vertragsärztinnen und Vertragsärzte zu übermitteln, datenschutzrechtlich gesehen keine Verbesserung darstellt. Der Personenbezug ist dadurch spätestens anlässlich von Arztbesuchen herstellbar. Geeignet wäre jedoch, die Staatsanwaltschaft einzuschalten, wenn tatsächliche Anhaltspunkte für eine Straftat, zum Beispiel nach § 263 Strafgesetzbuch (Betrug) oder § 29 Betäubungsmittelgesetz (Handel mit Betäubungsmitteln und anderem), vorliegen. Darüber hinaus haben wir angeregt, sich zu dieser Problematik mit den anderen Kassenärztlichen Vereinigungen im Zusammenwirken mit den Krankenkassen auszutauschen, um eine Orientierungshilfe zu erstellen. Daraufhin hat die KVHB erklärt, zukünftig auf Warnmeldungen zu verzichten und unsere Anregung zur Erarbeitung einer Orientierungshilfe für ihre Mitglieder aufzunehmen.

7.2 Nicht öffentlicher Bereich

7.2.1 Mängel bei der hausarztzentrierten Versorgung

Im Fünften Buch des Sozialgesetzbuches (SGB V) ist die hausarztzentrierte Versorgung geregelt. Danach sollen die Hausärztinnen und Hausärzte zunächst als Lotsin oder Lotse im Gesundheitssystem ihre daran teilnehmenden Patientinnen und Patienten behandeln. Hierbei ist auch eine Abrechung ohne die Beteiligung der Kassenärztlichen Vereinigungen vorgesehen. Das Bundessozialgericht hat im Jahr 2008 aufgrund der damals bestehenden Rechtslage die Einschaltung privater Stellen bei der Abrechnung ärztlicher Leistungen gegenüber den gesetzlichen Krankenkassen für unzulässig erklärt. Das Gericht betonte, dass hierbei ebenso detaillierte Regelungen über den Umfang der zu verarbeitenden Daten und über die erlaubten Datenflüsse vorliegen müssten, wie dies für klassische Abrechnungen über die Kassenärztlichen Vereinigungen der Fall ist. Es sei nicht nachvollziehbar, dass gerade bei der Einbeziehung von Privaten an diese geringere Anforderungen gestellt würden als an öffentlich-rechtliche Körperschaften (siehe auch Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17. und 18. März 2010 – Ziffer 19.1 dieses Berichts).

Daraufhin ist im SGB V eine Regelung geschaffen worden, die die Datenübermittlung von Versorgungszentren, die nicht mit der Kassenärztlichen Vereinigung abrechnen, an die jeweilige Krankenkasse erlaubt. Außerdem erlaubt sie unter anderem den Ärztinnen und Ärzten, auch private Dienstleister mit der Verarbeitung von Patientendaten zu Abrechnungszwecken zu beauftragen. Aufsicht über diese Auftragsdatenverarbeitung haben nach dem SGB V die Aufsichtsbehörden nach dem Bundesdatenschutzgesetz. Diese gesetzlichen Regelungen erfüllen die Anforderungen des Bundessozialgerichts an eine detaillierte Regelung nicht.

Im Frühjahr 2010 hat uns die Allgemeine Ortskrankenkasse (AOK) Bremen/Bremerhaven über erhebliche Datenschutzmängel unterrichtet, die in einem Vertragswerk mit dem Hausärzteverband (HÄV) Bremen und der Hausärztlichen Vertragsgemeinschaft (HÄVG) in Köln enthalten sind. Die Bedenken der AOK teilen wir, weil das Vertragswerk gegen wesentliche Elemente der Auftragsdatenverarbeitung in folgender Weise verstößt:

Einerseits sind die Hausärztinnen und Hausärzte an dem Rahmenvertrag, der das Verhältnis zwischen dem HÄV Bremen und der HÄVG festlegt, nicht beteiligt. Darin werden die Ärztinnen und Ärzte gezwungen, auf ihren Praxissystemen Software nach den Vorgaben des Hausärzteverbands zu installieren. Ihnen wird sogar vertraglich verboten, Kenntnis von wesentlichen Elementen der Software zu nehmen. Dadurch haben sie faktisch keine vollständige Kontrolle mehr über die Daten auf ihren Systemen. Insoweit würden sie nicht nur ihre Datenschutzpflichten, sondern auch ihre ärztliche Schweigepflicht verletzen. Ein Auftragsverhältnis ist andererseits rechtlich ausgeschlossen, da der HÄV, der ausschließlich nach Weisung der einzelnen Ärztinnen und Ärzte die Daten verarbeiten müsste, ein eigenes Interesse an diesen Daten hat. Insgesamt betrachtet hat die Hausärztin oder der Hausarzt die Wahl, entweder das gesamte Vertragswerk uneingeschränkt hinzunehmen oder

nicht an der hausarztzentrierten Versorgung teilzunehmen. Damit wird das Auftragsverhältnis unzulässigerweise auf den Kopf gestellt.

Die AOK hat sich auch aus diesen Gründen gegen dieses Vertragswerk gewandt, sodass entsprechend der Regelung im SGB V ein Schiedsspruch ergangen ist. Inzwischen hatte das Unabhängige Datenschutzzentrum Schleswig-Holstein (ULD) gegenüber dem HÄV Schleswig-Holstein per Anordnung nach § 38 Bundesdatenschutzgesetz die Datenübermittlung an den dortigen HÄV untersagt. Die daraufhin erfolgte Klage auf aufschiebende Wirkung der Anordnung ist vor dem Verwaltungsgericht Schleswig-Holstein abgelehnt worden. Praktisch zeitgleich hat die AOK vor dem Sozialgericht Bremen gegen den Schiedsspruch geklagt und war dabei ebenfalls im Eilverfahren erfolgreich.

Beide Gerichte schätzten unter Verweis auf die Anordnung des ULD und unsere Stellungnahme gegenüber der AOK die Risiken für das informationelle Selbstbestimmungsrecht der Patientinnen und Patienten beziehungsweise Versicherten höher ein als die Interessen der beiden Hausärzteverbände.

Bereits unmittelbar nach der Anordnung des ULD haben wir den HÄV Bremen aufgefordert, das Vertragswerk zur Vermeidung aufwändiger Parallelverfahren in den einzelnen Bundesländern bis zur Klärung der beiden Gerichtsverfahren auszusetzen und auf die Datenverarbeitung zu verzichten. Darüber hinaus haben wir das Gleiche einer Vielzahl von Krankenkassen auf deren Anfragen mitgeteilt. Diese Krankenkassen haben nämlich auf der Grundlage gleichlautender Vertragswerke mit Hausärztinnen und Hausärzten in Bremen abzurechnen. Auch die Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales, die die Aufsicht über die Krankenkassen führt, haben wir auf deren Wunsch unterrichtet.

Keine Bedenken würden bestehen, wenn entweder die zuständige Krankenkasse oder die zuständige Kassenärztliche Vereinigung als Auftraggeberin zur Abrechnung im Rahmen der hausarztzentrierten Versorgung im Wege der Auftragsdatenverarbeitung unter Einhaltung der gesetzlichen Bestimmungen hierzu andere Stellen mit entsprechenden Datenverarbeitungsvorgängen beauftragen würde.

In einer weiteren Instanz hat im Januar 2011 das Schleswig-Holsteinische Oberverwaltungsgericht (OVG) vollständig die Auffassung der Aufsichtsbehörde für den Datenschutz in Schleswig-Holstein unterstützt. Darüber hinaus hat das OVG erhebliche Zweifel an der Einhaltung der für eine Auftragsdatenverarbeitung nach den entsprechenden Vorschriften im SGB V und maßgeblichen Vorgaben in § 80 Absatz 5 SGB X. Danach liege es nämlich nicht auf der Hand, ob Störungen im Betriebsablauf bei Nichteinschaltung eines privaten Abrechnungsdienstleisters auftreten können. Zudem sei ein Kostenvergleich für das Vorliegen des § 80 Absatz 5 SGB X nicht vorgetragen worden.

Wir kommen aufgrund des OVG-Urteils zu dem Ergebnis, dass das gesamte die Auftragsdatenverarbeitung betreffende Vertragswerk mit dem Hausärzteverband Bremen grundlegend neu entwickelt werden muss. Unabdingbare Voraussetzung der hier in Rede stehenden Auftragsdatenverarbeitung wäre neben den bereits genannten Mängeln insbesondere, dass die Voraussetzungen der vom OVG besonders erwähnten Ausnahmeregelung § 80 Absatz 5 SGB X vorliegen. Mit hoher Wahrscheinlichkeit ist zu erwarten, dass das Hauptsacheverfahren zugunsten der Aufsichtsbehörde für den Datenschutz in Schleswig-Holstein ausgehen wird.

Daher haben wir den Hausärzteverband Bremen gebeten, das vorliegende Vertragswerk bis zur Klärung des Verfahrens in der Hauptsache auszusetzen. Außerdem soll der Verband seine Hausärzte, die daran beteiligt sind, darüber unterrichten, dass eine Übermittlung von Patientendaten weder an den Hausärzteverband noch an die Hausärztliche Vertragsgemeinschaft zulässig ist. Die Krankenkassenverbände und die Krankenkassen, die uns seinerzeit um Stellungnahme gebeten hatten, haben wir entsprechend unterrichtet, ebenso die Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales.

7.2.2 Zuständigkeitswechsel bei der Datenschutzkontrolle über die Grundsicherung für Arbeitssuchende

Nach dem Gesetz zur Weiterentwicklung der Organisation der Grundsicherung für Arbeitssuchende wird die Zuständigkeit für die Datenschutzkontrolle für die gemeinsamen Einrichtungen der Bundesagentur für Arbeit und der Kommunen auf den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) übertragen. Der Wechsel in der Zuständigkeit gilt ab dem 1. Januar 2011. Betrof-

fen sind davon die Datenschutzkontrollen über die Bremer Arbeitgemeinschaft für Integration und Soziales (BAgIS) und die Arbeitsgemeinschaft (ARGE) JobCenter Bremerhaven. Grund für die jetzt geänderte verteilte Zuständigkeit war im Wesentlichen, dass die Bundesagentur einerseits für die Datenverarbeitungssysteme in den gemeinsamen Einrichtungen verantwortlich war und die Einrichtungen vor Ort die Zuständigkeit für die Datenverarbeitung hatten. Entsprechend war auch die Datenschutzkontrolle geregelt. Mehr oder weniger regelmäßig hatten wir Beschwerden, die im Zusammenhang mit dem Datenverarbeitungssystem zusammenhingen, die dann an den BfDI abzugeben waren.

Der Zuständigkeitswechsel hat den Vorteil, dass nunmehr die Datenschutzkontrolle in einer Hand liegt, nämlich beim Bundesdatenschutzbeauftragten. Gleichwohl ist zu befürchten, dass die räumliche Distanz zu den Behörden dazu führen kann, dass die Beschwerden und Eingaben bei der Datenverarbeitung in den gemeinsamen Einrichtungen nicht so zeitnah bearbeitet werden können wie bisher. Wir konnten in Schulungsveranstaltungen und Beratungsgesprächen mit der BAgIS und dem JobCenter ein gutes Datenschutzniveau vor Ort erreichen, sodass die Beschwerden in der letzten Zeit deutlich zurückgegangen sind. Es bleibt zu hoffen, dass den Anliegen der Betroffenen mit der neuen Zuständigkeitsregelung in gleicher Weise Rechnung getragen werden wird.

8. Bildung

8.1 Erhebung von Diagnosedaten zur Bescheinigung der Prüfungsfähigkeit von Lehramtskandidatinnen und Lehramtskandidaten

Das Formular über die Bescheinigung der Prüfungsfähigkeit von Lehramtskandidatinnen und Lehramtskandidaten enthielt Angaben über Krankheiten und den Grad psychischer Erkrankungen. Auf Anfrage hat die Senatorin für Bildung und Wissenschaft zur Begründung dieser Praxis auf ein Urteil des Bundesverwaltungsgerichts vom 6. August 1996, Aktenzeichen 6 B 17/96, verwiesen. Danach beschränkt sich die ärztliche Beteiligung jedoch nur darauf, krankhafte Beeinträchtigungen zu beschreiben und darzulegen, welche Auswirkungen sie auf das Leistungsvermögen des Prüflings in der konkret abzulegenden Prüfung habe.

Aus diesen Gründen halten wir es für datenschutzrechtlich geboten, dass nur diese Angaben in der ärztlichen Bescheinigung enthalten sind. Aus dem Attest dürfen demnach nur die Hindernisse für die Teilnahme an der Prüfung hervorgehen, wie die Anordnung einer notwendigen Bettruhe, die objektive Unfähigkeit, sich ohne erhebliche Beschwerden oder sich, ohne die Krankheitserscheinungen zu verschlimmern, zum Ort der Prüfung zu begeben und sich dort der Prüfung zu unterziehen. Das Attest darf keine medizinischen Diagnosen enthalten. Es sollte sich daraus nur ergeben, ob aus ärztlicher Sicht Prüfungsunfähigkeit anzunehmen ist. Mittlerweile ist das Formular entsprechend geändert worden, sodass es insbesondere keine Diagnosen und auch nicht den Grad der psychischen Erkrankung enthält.

Unabhängig davon sind auch die rechtmäßig enthaltenen Gesundheitsdaten, deren Erhebung ausdrücklich gesetzlich erlaubt werden muss, was bisher nicht der Fall war. Wir haben daher das Bildungsressort gebeten, auf eine entsprechende Ergänzung des Bremischen Lehrerausbildungsgesetzes hinzuwirken. Die Senatorin für Bildung und Wissenschaft hat unseren Vorschlag aufgenommen. Die gesetzliche Neuregelung ist Ende des Jahres 2010 in Kraft getreten.

8.2 Richtlinien zur Führung von Schullaufbahnakten

Das Bremische Schuldatenschutzgesetz ist im Jahr 2007 grundlegend geändert worden. Dies hat zur Folge, dass die Richtlinien zur Führung von Schullaufbahnakten der Gesetzesänderung angepasst werden müssen. Die Senatorin für Bildung und Wissenschaft hat zugesagt, das Verfahren zur Anpassung der Richtlinien kurzfristig einzuleiten und erklärt, uns über den Entwurf rechtzeitig zu unterrichten. Eine Unterrichtung ist bisher nicht erfolgt.

8.3 Veröffentlichung von Schülerdaten und Fotos über Schülerinnen und Schüler im Internet

Eine Schule hat unsere Anfrage aufgrund einer Elterneingabe zur Veröffentlichung von Schülerdaten und Fotos über Schülerinnen und Schüler auf der schuleigenen Internetseite an die Senatorin für Bildung und Wissenschaft abgegeben.

Die Behörde hat auf unsere Anfrage erklärt, die Überarbeitung der Einwilligungserklärung zur Verwendung und Veröffentlichung von Personenabbildungen von Schülerinnen und Schülern auf Internetseiten der Schulen werde kurzfristig eingeleitet. Des Weiteren ist zugesagt worden, uns über den Entwurf zu unterrichten.

Wir haben die senatorische Dienststelle darauf hingewiesen, dass wir hierzu bereits einige Schulen beraten haben, die daraufhin die entsprechenden Einwilligungserklärungen überarbeitet hatten. Hierbei sind unsere Vorschläge aufgenommen worden, die vielen Elternwünschen nach einer differenzierten Einwilligungserklärung entsprechen. Danach können die Eltern einwilligen, dass die Schule Fotos, Texte und Zeichnungen mit oder ohne vollständige oder nur Vornamensnennung oder nur Teile davon im Internet und/oder in Zeitungsartikeln veröffentlicht. Diese Differenzierung ist erforderlich, weil die Auswirkungen der unterschiedlichen Veröffentlichungen gravierend sind. Im Gegensatz zur Presse können im Internet die Daten und Bilder jederzeit von jeder Nutzerin und jedem Nutzer des Internet an jedem Ort in vielfältiger Weise verarbeitet, verknüpft oder verfälscht werden.

Erst nach Hinweisen von Schulen sind wir auf eine Verfügung der Senatorin für Bildung und Wissenschaft aufmerksam geworden. Diese erfüllt in keiner Weise die vorgenannten Anforderungen einer differenzierten Einwilligung. Daher haben wir die senatorische Behörde gebeten, eine Einwilligungserklärung zu erstellen, die das differenzierte Wahlrecht der Eltern gewährleistet. Daraufhin hat die Senatorin für Bildung und Wissenschaft die Einwilligungserklärung entsprechend überarbeitet.

9. Umwelt und Bau

9.1 Vertraulichkeit des Anzeigenaufgebers

Im Berichtszeitraum wandte sich ein Ehepaar an uns und teilte mit, dass sie sich in einem Schreiben an den Senator für Umwelt, Bau, Verkehr und Europa gewandt und auf den Betrieb eines Gästehauses in einer Wohnstraße hingewiesen hätten. Dabei hätten sie darum gebeten, die Informationen vertraulich zu behandeln, um sich vor eventuellen Reaktionen der Betreiber des Gästehauses zu schützen. Inzwischen sei ihnen bekannt geworden, dass der Senator an den Betreiber des Gästehauses herangetreten sei. Trotz ihrer Bitte sei ihr Name nicht geheim gehalten worden. Auf unsere Anfrage beim Senator für Umwelt, Bau, Verkehr und Europa wurde mitgeteilt, dass die vertrauliche Behandlung der Daten bei einer erfolgten Akteneinsicht nicht beachtet worden sei.

Wenn ein Beschwerdeführer es ausdrücklich wünscht, hat er grundsätzlich ein Recht darauf, dass sein Name aus bestimmten Gründen nicht bekannt gegeben wird. Dies ist zumindest dann der Fall, wenn es für den Entschluss über ein behördliches Einschreiten nicht entscheidend auf eine tatsächliche Betroffenheit des Beschwerdeführers ankommt. Die Abteilungsleitung beim Senator für Umwelt, Bau, Verkehr und Europa hat diesen Vorgang zum Anlass genommen, den Verfahrensablauf von Nachbarschaftsbeschwerden künftig so zu organisieren, dass die Wahrung der Anonymität – sofern dies ausdrücklich gewünscht wird – gewährleistet wird. Wir gehen daher davon aus, dass die senatorische Dienststelle zukünftig in gleich gelagerten Fällen die Anonymität der Beschwerdeführenden wahrt.

9.2 Anpassung des Bremischen Wassergesetzes an das Wasserhaushaltsgesetz

Das Recht der Wasserwirtschaft ist seit der Föderalismusreform 2006 neu geregelt. Dem Bund obliegt nun die Möglichkeit, im Bereich des Wasserhaushalts Vollregelungen zu erlassen. Im Rahmen der sogenannten Abweichungsgesetzgebung dürfen die Länder durch eigene Rechtsvorschriften vom Bundesrecht abweichen. Das neue Wasserhaushaltsgesetz trat am 1. März 2010 in Kraft. Da das Bremische Wassergesetz entsprechend angepasst werden sollte, wurden wir um Stellungnahme gebeten. Es war vorgesehen, neben der im Wasserhaushaltsgesetz enthaltenen Regelung zum Umgang mit personenbezogenen Daten keine weitere Vorschrift der Informationsbeschaffung und -übermittlung in das Bremische Wassergesetz aufzunehmen. Nach einem Vergleich der entsprechenden Vorschrift im neuen Wasserhaushaltsgesetz mit der bestehenden Regelung im Bremischen Wassergesetz stellten wir fest, dass die letztgenannte Norm nach Inkrafttreten des neuen Wasserhaushaltsgesetzes teilweise entbehrlich sein wird. Wir wiesen jedoch darauf hin, dass anlässlich einer vor wenigen Jahren erfolgten Anpassung des Bremischen

Wassergesetzes an Vorgaben der Europäischen Union auf unser Drängen hin die wesentlichen Betroffenengruppen mit aufgeführt wurden, deren personenbezogene Daten im Rahmen des Wassergesetzes verarbeitet werden dürfen. Hintergrund unserer Forderung war der verfassungsrechtlich gebotene Grundsatz der Normenklarheit. Diese Klarstellung sollte durch die Anpassung des Bremischen Wassergesetzes nicht entfallen. Zudem enthält das Wasserhaushaltsgesetz im Gegensatz zur alten Fassung des Bremischen Wassergesetzes keine Regelung zur Einsicht durch jedermann. Wir baten daher um Übernahme der bisherige Regelung zur Einsichtnahme in das Wasserbuch in die Neufassung des Bremischen Wassergesetzes. Unseren Forderungen wurde in vollem Umfang entsprochen, sodass wir gegen den Gesetzentwurf keine Bedenken hatten.

9.3 Veröffentlichung eines Solarkatasters im Internet

Zum Zweck der Verbreitung von Photovoltaikanlagen und thermischen Solaranlagen auf Dach- und Gebäudeflächen plant die Stadt Bremerhaven die Errichtung und Veröffentlichung eines Dachflächenkataster „Sun-Area Bremerhaven“ im Internet. Das Kataster soll Auskunft über die Eignung der Dachflächen einzelner Gebäude zur Strom- und Wärmeerzeugung geben. Die dafür notwendigen Daten wie Form, Neigung und Höhe von Dach- und Geländeflächen wurden bereits im Rahmen von Messflügen erhoben. Unter Eingabe einer Straße und Hausnummer soll über das Internet für jedes Dach die jeweilige Eignungsstufe für die Errichtung von Solaranlagen festgestellt werden können. Die verschiedenen Eignungsstufen werden dafür in unterschiedlichen Farben dargestellt. Es handelt sich bei diesen Informationen um personenbezogene Daten, weil ohne besonderen Aufwand an Zeit, Kosten und Arbeitskraft über die Straße und Hausnummer ein Bezug zu bestimmten natürlichen Personen (zum Beispiel Eigentümer, Erbbauberechtigte und Bewohner) über Telefonbücher, elektronische Adress- und Telefonverzeichnisse im Internet sowie sonstige Internetsuchmaschinen et cetera herstellbar ist. Eine Veröffentlichung dieser Daten im Internet ist nicht ohne Weiteres zulässig, denn dadurch würden schutzwürdige Belange der Eigentümer und Erbbauberechtigten erheblich beeinträchtigt werden, weil ihre Daten über Internetsuchmaschinen weltweit von jeder Person in vielfältiger Weise verknüpft und verfälscht werden können. Die Veröffentlichung von personenbezogenen Daten im Internet beinhaltet eine ungleich höhere Eingriffsintensität für die Betroffenen als eine Veröffentlichung der Daten in gedruckter Form, da die Daten einfach recherchierbar, unbeschränkt abrufbar und beliebig mit anderen Daten verknüpfbar sind. Bei einmal eingestellten Daten ist es für den Betroffenen aufgrund der unkontrollierbaren Vervielfältigung im Netz faktisch nicht möglich, eine Löschung oder Berichtigung zu erreichen. In seiner Antwort auf die Kleine Anfrage der Fraktion der FDP (Freie Demokratische Partei) zum Dachflächenkataster „Sun-Area Bremerhaven“ vom 29. Juni 2010 teilt der Senat die Rechtsauffassung der Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI), wonach öffentliche Stellen personenbezogene Daten im Internet nur unter der Voraussetzung veröffentlichen dürfen, dass eine Rechtsgrundlage diese Veröffentlichungsform ausdrücklich mit einbezieht oder die Einwilligung der Betroffenen vorliegt. Wie die LfDI ist der Senat der Auffassung, dass eine Rechtsgrundlage, die die Veröffentlichung im Internet vorsieht, im Fall des Solarkatasters nicht gegeben ist.

In einer gemeinsamen Besprechung im Herbst 2010 zwischen unter anderem den Amtsleitungen des Vermessungs- und Katasteramts Bremerhaven und des Umweltschutzamts Bremerhaven, der die Software entwickelnden Stelle, der das Projekt finanzierenden Firma und uns wurde eine datenschutzgerechte Lösung entwickelt. Danach kann die Dateiansicht für die Solaranalysepotenzialdaten einer Immobilie nur mit Hilfe einer Zugangsberechtigung geöffnet werden. So können nur die Eigentümerin oder der Eigentümer selbst, nicht aber beliebige andere Personen die entsprechenden Informationen über ihr oder sein Gebäude erhalten. Die Zugangsberechtigung könnte beispielsweise über die Grundsteuerbescheidnummer oder die Flurstücksbezeichnung laufen. Seitens des Magistrats der Stadt Bremerhaven wurde zugesichert, die Lösung zu prüfen.

Aus der Presse erfuhren wir zwischenzeitlich, dass der Magistrat der Stadt Bremerhaven die Veröffentlichung des Dachflächenkatasters im Internet beschlossen hat. Zunächst gingen wir davon aus, dass es sich hierbei um die gemeinsam erarbeitete Lösung handelte. Nach der Presseberichterstattung Anfang des Jahres 2011 scheint dies jedoch nicht der Fall zu sein. Am 7. Februar 2011 soll das Solarkataster

in unveränderter Form in das Internet gestellt werden. An die Stelle der bei Veröffentlichungen von öffentlichen Stellen gesetzlich geforderten vorherigen Einwilligung tritt in Bremerhaven ein Widerspruchsrecht à la Google Street View. Schon die jetzt bei uns eingegangenen Eingaben zeigen, dass das Solarkataster auch im nächsten Jahresbericht Thema werden wird.

10. Finanzen und Verwaltungsmodernisierung

10.1 Zustellung des Steuerbescheids per Post in einem mit Tesafilm verschlossenen Briefumschlag

Im März des Berichtsjahrs teilte uns ein Steuerpflichtiger mit, er habe am 3. März 2010 seinen auf den 25. Februar 2010 datierten Steuerbescheid vom Finanzamt Bremen-West per Post erhalten. Der Briefumschlag sei jedoch nicht mehr original verklebt gewesen, sondern er sei mit Tesafilm verschlossen worden.

Aufgrund unserer Anfrage teilte das Finanzamt Bremen-West mit, dass der Steuerbescheid als Brief im Rahmen des Zentralversandes zur Post aufgegeben worden sei. Hierbei werden die Bescheide zentral durch das Dataport-Druckzentrum in Altenholz erstellt und kuvertiert, per Transporter nach Bremen gebracht und hier bei Performa Nord durch eine Frankiermaschine frankiert und dann an die Post ausgeliefert. Das Finanzamt sei somit mit der Absendung des Bescheids nicht befasst gewesen.

Daraufhin wandten wir uns zur weiteren Sachverhaltsaufklärung an Dataport. Hier wurde uns geschildert, dass aufgrund der Technik der Kuvertiermaschine niemals Tesafilm zum Verschließen von Briefumschlägen verwendet werde. Wenn es zu Problemen mit der Kuvertiermaschine komme, sei weder das zu kuvertierende Schriftgut noch der Umschlag weiter verwendbar. Das Schriftgut werde in solchen Fällen nachgedruckt und die Kuvertierung erfolge wiederum durch die Kuvertiermaschine. Letztlich baten wir auch Performa Nord um eine Stellungnahme. Von dort wurde uns mitgeteilt, dass, wenn im Rahmen der Frankierung ein Briefumschlag beschädigt werde, dieser nicht mit Tesafilm geflickt, sondern durch einen neuen Umschlag ersetzt werde.

Anhand der eingegangenen Stellungnahmen konnten unsererseits keine Anhaltspunkte dafür festgestellt werden, dass der Briefumschlag bei Dataport oder Performa Nord mit Tesafilm verschlossen wurde oder eine unbefugte Einsichtnahme der im Steuerbescheid enthaltenen Daten stattgefunden hat. Ebenso konnten keine offensichtlich erkennbaren Fehlerquellen bei der Kuvertierung und Versendung von Steuerbescheiden erkannt werden.

10.2 Einrichtung einer zentralen Zuwendungsdatenbank

Die bremischen Senatsressorts und beliehenen Unternehmen gewähren regelmäßig staatliche Zuwendungen an private Einrichtungen, die öffentliche Aufgaben außerhalb der Verwaltung wahrnehmen (vergleiche zur Veröffentlichung eines Zuwendungsberichts Ziffer 2.6 des 5. Jahresberichts der Landesbeauftragten für Informationsfreiheit). Da bei der Überprüfung der Zuwendungen durch den Rechnungshof des Landes Bremen in der Vergangenheit Mehrfachförderungen festgestellt worden waren, wurde der Ruf nach einer zentralen Zuwendungsdatenbank laut. An eine solche einheitliche Datenbank sollen alle bremischen Behörden, Eigenbetriebe sowie beliehene Gesellschaften angeschlossen werden. Dadurch entfällt die Notwendigkeit, ressortspezifische Lösungen zu entwickeln und zu betreiben. Mit Hilfe der zentralen Zuwendungsdatenbank können die zuwendungsgebenden Stellen überprüfen, ob eine antragstellende Einrichtung bereits von anderer Seite Zuwendungen erhalten hat. So sollen Mehrfachförderungen vermieden, Transparenz geschaffen und die Erstellung des jährlichen Zuwendungsberichts dadurch vereinfacht werden.

In einem gemeinsamen Termin mit der Senatorin für Finanzen haben wir unsere datenschutzrechtlichen Anforderungen an die Erstellung einer zentralen Zuwendungsdatenbank dargelegt und auf die Notwendigkeit der Erstellung eines Datenschutzkonzepts hingewiesen. Eine Entwurfsfassung, zu der wir Stellung genommen haben, wurde uns bereits von der Senatorin für Finanzen vorgelegt. Ergänzungsbedarf gibt es bei den technischen und organisatorischen Maßnahmen. Dies gilt insbesondere für das Rechte- und Rollenkonzept und das Antragsverfahren für Berechtigungen, für die Festlegung von Verantwortlichkeiten für Berechtigungen,

für den Support (Unterstützung) und die Administration (Verwaltung) des Verfahrens sowie die Eingabekontrolle. Datenschutzrechtlich relevant sind auch das Berichtswesen, die Altdatenübernahme und die Schnittstelle zum SAP. Wir erwarten hier eine zügige Fortschreibung der Datenschutzdokumentation und werden das Projekt weiterhin bis zum Abschluss begleiten.

10.3 Berechnung der Pensionsrückstellungen im Rahmen der Eröffnungsbilanz

Im Zuge der Reform des Haushaltswesens wollte das Land Bremen erstmalig zum Stichtag 1. Januar 2010 eine Bilanz nach kaufmännischen Grundsätzen erstellen. Das Projekt, das eine transparente Ausweisung der Vermögenslage bezweckt, ist bei der Senatorin für Finanzen angesiedelt. Den Personalkosten und damit verbundenen Pensionsrückstellungen kommt dabei eine große Bedeutung zu. Durch die Bildung von Pensionsrückstellungen wird die Belastung zukünftiger Rechnungsperioden deutlich. Die finanziellen Verpflichtungen gegenüber Pensions- und anderen Leistungsberechtigten beeinflussen den Rahmen zukünftiger Haushaltsjahre. Für die Berechnung der Pensionsrückstellungen, die nach wissenschaftlich fundierten Methoden erfolgt, werden personenbezogene Daten der Beschäftigten der Freien Hansestadt Bremen benötigt. Die erforderlichen Daten sind bereits in bestehenden Verfahren vorhanden. Wir teilten der Senatorin für Finanzen mit, dass wir eine Verwendung der Daten für die Berechnung nur dann für zulässig halten, wenn eine entsprechende Rechtsgrundlage dies erlaubt. Da zum damaligen Zeitpunkt noch keine derartige Regelung existierte, schlugen wir vor, im Haushaltsgesetz der Freien Hansestadt Bremen für das Haushaltsjahr 2010 eine solche Norm zu schaffen. Das ist geschehen. Durch die betreffende Norm wird die Senatorin für Finanzen nun ermächtigt, zur Berechnung von Pensionsrückstellungen und ähnlichen Verpflichtungen der Freien Hansestadt Bremen die dafür notwendigen Daten aus den entsprechenden Verfahren unter Berücksichtigung datenschutzrechtlicher Vorschriften zu verarbeiten.

Da es sich bei den benötigten Informationen um sensible Beschäftigtendaten handelt, waren wir bei der Durchführung der Berechnung mit vor Ort. Dabei konnten wir uns davon überzeugen, dass ein datenschutzkonformer Umgang mit den Informationen erfolgte. Allerdings war das Datenschutzkonzept zum Verfahren der Berechnung der Pensionsrückstellungen bisher unvollständig. Es fehlte insbesondere noch eine Beschreibung der vom Bremischen Datenschutzgesetz geforderten technischen und organisatorischen Maßnahmen. In der Zwischenzeit wurde uns eine überarbeitete Fassung vorgelegt. Auch diese Beschreibung erfüllt unsere Anforderungen nicht.

10.4 Telefonisches Bürger-Service-Centrum/D115

Im 32. Jahresbericht unter Ziffer 10.5 berichteten wir über eine Telefonverkehrsmessung, die im Vorfeld des Projekts „Telefonisches Bürger-Service-Centrum/D115“ stattgefunden hat. Im Berichtszeitraum haben wir das bei der Senatorin für Finanzen angesiedelte Projekt weiter begleitet. Der Senat möchte mit dem Vorhaben seinen telefonischen Bürgerservice verbessern und, damit einhergehend, die Voraussetzungen für einen Beitritt Bremens zum nationalen D115-Verbund schaffen. Das Projekt D115 verfolgt das Ziel, Bürgerinnen und Bürgern unter einer einheitlichen Servicebehördenrufnummer eine direkte Verbindung in die Verwaltung zu bieten. Dabei spielt es keine Rolle, welche Verwaltungsebene, konkrete Behörde oder Dienststelle für das jeweilige Anliegen zuständig ist. In einer Stellungnahme zu den bisherigen Projektunterlagen haben wir darauf hingewiesen, dass insbesondere der Umgang mit den Daten der Anruferinnen und Anrufer noch abschließend geklärt und dokumentiert werden muss. Hinsichtlich eines geplanten Statistikmoduls muss ausgeschlossen werden, dass mittels der anfallenden Daten eine Leistungs- und Verhaltenskontrolle der Mitarbeiterinnen und Mitarbeiter erfolgen kann. Für die elektronische Übermittlung von personenbezogenen Daten sind sichere Kommunikationswege einzurichten. Nach den Vorschriften des Bremischen Datenschutzgesetzes (BremDSG) ist für das Projekt ein Datenschutzkonzept zu erstellen, das den sicheren Umgang mit personenbezogenen Daten dokumentiert. Es ist dem behördlichen Datenschutzbeauftragten zur Vorabkontrolle vorzulegen.

Für das IT-System Bürgerservice sollen aus verschiedenen Systemen personenbezogene Daten zusammengeführt werden. Die Prozesse, die Zugriffsberechtigungen und die Maßnahmen zum Schutz der Daten sind im Datenschutzkonzept für das IT-System Bürgerservice darzustellen. Sofern darüber hinaus weitere Anwendun-

gen geplant sind, mit denen personenbezogene Daten verarbeitet werden, sind ebenfalls Verfahrensbeschreibung und Datenschutzkonzept nach § 7 und § 8 BremDSG zu erstellen.

Sobald uns das Konzept vorliegt, werden wir es auf Datenschutzkonformität überprüfen.

11. Medien

11.1 Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung

Das Bundesverfassungsgericht hat am 2. März 2010 die Vorratsdatenspeicherung für verfassungswidrig und damit nichtig erklärt. Nach den angegriffenen Regelungen zur Vorratsdatenspeicherung waren alle öffentlich zugänglichen Telekommunikationsanbieter verpflichtet, praktisch sämtliche Verkehrsdaten von Telefondiensten, E-Mail-Diensten und Internetdiensten vorsorglich anlasslos für sechs Monate zu speichern. Die Vorschriften sollten die Europäische Richtlinie 2006/24/EG umsetzen.

Der Erste Senat des Bundesverfassungsgerichts in Karlsruhe begründete seine Entscheidung damit, dass die Datensammlung des Staates in dieser Form gegen das Telekommunikationsgeheimnis verstoße. Die Karlsruher Richterinnen und Richter machen deutlich, dass es sich bei einer solchen Speicherung um einen besonders schweren Eingriff mit einer Streubreite handele, wie sie die Rechtsordnung bisher nicht kenne. Auch Verkehrsdaten würden inhaltliche Rückschlüsse bis in die Intimsphäre ermöglichen und damit aussagekräftige Persönlichkeits- oder Bewegungsprofile liefern. Weil keine ausreichende Datensicherheit gewährleistet sei und die Datenverwendung von den Bürgerinnen und Bürgern nicht bemerkt werde, sei die Vorratsdatenspeicherung in ihrer bisherigen Form geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen könne.

Unter einer Reihe enger Vorgaben soll eine Vorratsdatenspeicherung nach Auffassung des Bundesverfassungsgerichts allerdings weiterhin möglich sein. Zu diesen Vorgaben gehören unter anderem die Gewährleistung eines besonders hohen Standards der Datensicherheit und das Vorliegen von schwerwiegenden Straftaten. Aus Sicht des Datenschutzes wäre es wünschenswert gewesen, wenn das Bundesverfassungsgericht noch weiter gegangen wäre und eine anlasslose Massenspeicherung von Verkehrsdaten grundsätzlich für nicht mit dem deutschen Verfassungsrecht vereinbar erklärt hätte.

Auch die Datenschutzbeauftragten des Bundes und der Länder haben sich nach dem Urteil auf ihrer 79. Konferenz am 17. und 18. März 2010 erneut grundsätzlich ablehnend in ihrer Entschließung „Keine Vorratsdatenspeicherung!“ (vergleiche Ziffer 19.4 dieses Berichts) gegen die Vorratsdatenspeicherung ausgesprochen und die Bundesregierung aufgefordert, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen.

Es bleibt zu hoffen, dass die nicht nur innerhalb der Bundesregierung kontrovers geführte Diskussion hinsichtlich der Schaffung neuer Vorratsdatenspeicherungsregelungen zugunsten der Persönlichkeitsrechte der Bürgerinnen und Bürger entschieden wird. Von der Bundesjustizministerin wird eine verdachtsunabhängige Protokollierung von Nutzerspuren ausgeschlossen.

11.2 Neues Rundfunkgebührenmodell

Am 15. Dezember 2010 haben die Ministerpräsidenten der Länder den 15. Rundfunkänderungsstaatsvertrag unterzeichnet. Die bisherige an den Besitz eines Empfangsgeräts gekoppelte Rundfunkgebühr wird durch die Erhebung eines an das Innehaben einer Wohnung oder Betriebsstätte angeknüpften Beitrages ersetzt. Ziel des neuen Beitrags soll neben einer höheren Beitragsgerechtigkeit auch eine deutlich datenschutzgerechtere Beitragserhebung sein. Hinsichtlich der Verwirklichung des letztgenannten Ziels hatten die Datenschutzbeauftragten des Bundes und der Länder Zweifel und aus diesem Grund zu den Entwürfen des Staatsvertrages umfassend Stellung genommen sowie am 15. September 2010 in einer Entschließung auf die datenschutzrechtlichen Bedenken hingewiesen (vergleiche Ziffer 19.8 dieses Berichts). Kritisiert wurden in erster Linie die weiterhin bestehenden umfangreichen Erhebungsbefugnisse der Rundfunkanstalten.

Einer der kritisierten Punkte ist und bleibt die Datenerhebung bei Adresshändlern durch die Rundfunkanstalten. Das Beschaffen von Adressdaten aus privaten Quellen durch öffentliche Stellen wurde ohnehin schon immer von den Datenschutzaufsichtsbehörden als unverhältnismäßig abgelehnt (vergleiche 27. Jahresbericht, Ziffer 2.2). Nach der Umstellung von der Geräteabgabe auf eine Wohnungsabgabe ist der Ankauf von Adressdaten erst recht nicht mehr erforderlich. Auf die datenschutzrechtlichen Bedenken diesbezüglich wurde insoweit eingegangen, als in die Übergangsvorschriften die Regelung „Die Landesrundfunkanstalten dürfen bis zum 31. Dezember 2014 keine Adressdaten privater Personen ankaufen." aufgenommen wurde. Wünschenswert wäre allerdings die komplette Streichung dieser Erhebungsbefugnis gewesen.

Aufgrund der datenschutzrechtlichen Bedenken wurde die Übermittlung der Meldebehörde an die Rundfunkanstalten überarbeitet. Nunmehr wird der einmalige Meldedatenabgleich nicht, wie vorgesehen, innerhalb von zwei Jahren ab Inkrafttreten des Staatsvertrages erfolgen, sondern an einem bundeseinheitlichen Stichtag vorgenommen. Die Daten sollen an dem Stichtag eingefroren werden. In der Stellungnahme der Datenschutzbeauftragten war allerdings gefordert worden, auf die pauschale Datenübermittlung grundsätzlich zu verzichten. Stattdessen war vorgeschlagen worden, die Datenübermittlung auf zeitnahe Übermittlungsbefugnisse nach dem Melderecht zu beschränken.

Auch andere datenschutzrechtliche Forderungen blieben unberücksichtigt. Hierzu gehört zum Beispiel die von den Datenschutzbeauftragten formulierte Forderung, bei Befreiungsanträgen aus sozialen Gründen, wie Armut oder Behinderung, nur die Vorlage einer Bestätigung des Leistungsträgers zuzulassen und auf die Vorlage der vollständigen Leistungsbescheide zu verzichten.

11.3 Verschlüsselung von Nutzerkonten

Im Berichtsjahr haben wir Onlinezugänge zu Nutzerkonten öffentlicher Bibliotheken auf ihre Datensicherheit überprüft.

Bibliotheken mit einem Onlineangebot sind Diensteanbieter nach dem Telemediengesetz (TMG). Gemäß § 13 Absatz 4 Nummer 3 TMG muss jeder Diensteanbieter durch technische und organisatorische Maßnahmen sicherstellen, dass die Nutzerinnen und Nutzer Telemedien gegen die Kenntnisnahme Dritter geschützt in Anspruch nehmen können. Dies gilt auch für den Zugang zu den Nutzerkonten. Bei fehlender Verschlüsselung können sich Unberechtigte die Zugangsdaten verschaffen und Einsicht in die Nutzerkonten nehmen. Aus der Auswahl und der Zusammenstellung der Literatur ergeben sich Profile über die Kontoinhaberinnen und Kontoinhaber, welche vor der unberechtigten Einsichtnahme geschützt sein sollten.

Bei den von uns angeschriebenen Bibliotheken wird der Zugriff auf die Nutzerkonten jetzt neben einer unverschlüsselten Verbindung auch mittels verschlüsselte SSL-Verbindung (Secure Sockets Layer, Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet) angeboten. Alle Nutzerinnen und Nutzer sollten von der verschlüsselten Verbindung zum eigenen Schutz auch Gebrauch machen.

11.4 Versendung von E-Mails an Personengruppen

Im Berichtsjahr erhielten wir eine Beschwerde über eine Einrichtung, die Betreuungspersonen vermittelt. Die Einrichtung hatte die Betreuungspersonen per E-Mail mit einem offenen Verteiler angeschrieben, sodass jede der angeschriebenen Personen jeweils die Namen der anderen Personen mit deren E-Mail-Adressen zur Kenntnis nehmen konnte.

Die Bekanntgabe der E-Mail-Adressen der anderen Betreuungspersonen war aus datenschutzrechtlicher Sicht schon nicht erforderlich, sodass die Übermittlung der Daten nur mit Einwilligung der Betroffenen rechtmäßig gewesen wäre. Wir haben der Einrichtung allerdings eine praktikablere Lösung vorgeschlagen. Setzt man den gesamten Verteiler in das Feld „bcc" (Blindkopie), wird dadurch die Kenntnisnahme von E-Mail-Adressen durch andere Adressaten verhindert.

Die Einrichtung hat uns mitgeteilt, dass sie alle Mitarbeiterinnen und Mitarbeiter auf das Datenschutzgesetz hingewiesen und sie über die korrekte, datenschutzrechtlich einwandfreie Durchführung der E-Mail-Versendung an Verteilergruppen informiert habe.

11.5 Datenschutzrichtlinie für elektronische Kommunikationsdienste: Opt-In-Lösung für Cookies

In der europäischen Datenschutzrichtlinie für elektronische Kommunikationsdienste wurden die datenschutzrechtlichen Voraussetzungen für elektronische Kommunikationsdienste neu festgelegt. Artikel 5 Absatz 3 der Richtlinie ersetzt die bisherige Opt-Out-Lösung (Widerspruchslösung) durch eine Opt-In-Lösung (Einwilligungslösung) mit einer vorherigen umfassenden Information über die Zwecke der Verarbeitung. Die Richtlinie muss im Frühjahr 2011 in nationales Recht umgesetzt werden. Dies macht eine Anpassung im Telemediengesetz (TMG) erforderlich. Im geltenden TMG ist in § 15 Absatz 3 eine Widerspruchslösung vorgesehen. Nunmehr muss eine informierte Einwilligung normiert werden.

Das zuständige Ministerium sieht schon im derzeitigen TMG in § 12 Absatz 1 und Absatz 2 die Einwilligungslösung realisiert und verlangt lediglich eine strengere Auslegung des Gesetzes. Die Datenschutzaufsichtsbehörden sehen hierin keine den Anbietern vermittelbare Lösung, da die bisherige Auslegung sich in der Praxis bewährt hat und allgemein anerkannt ist. Sie fordern daher in dem Beschluss des Düsseldorfer Kreises vom 24. und 25. November 2010 „Umsetzung der Datenschutzrichtlinie für elektronische Kommunikationsdienste“ (vergleiche Ziffer 20.5 dieses Berichts) eine eindeutige und klare gesetzliche Anpassung.

12. Beschäftigtendatenschutz

12.1 Veröffentlichung von Beschäftigtendaten und Fotos über Beschäftigte im Internet

Der Inhaber eines Einzelhandelsgeschäfts hatte auf seiner Internetseite in einem sogenannten Web-Log viele mit seinem Geschäft in Zusammenhang stehende Sachverhalte protokolliert, aufgezeichnet und zur Diskussion gestellt. Dabei wurde auch Fehlverhalten seiner Beschäftigten angeprangert. Die Veröffentlichungen erfolgten ohne Namensnennung. Angesichts der geringen Beschäftigtenzahl war es aber ohne besonderen Aufwand möglich, die betreffende Person zu identifizieren. Es befanden sich auch Fotos der Beschäftigten unter Angaben ihrer Vor- und Nachnamen auf der Internetseite. Zudem hatten die Leserinnen und Leser die Möglichkeit, diese Schilderungen zu kommentieren.

Auf unsere Anfrage hat der Inhaber erklärt, die mündliche Einwilligung in die Veröffentlichung der Fotos und Namen seiner Beschäftigten habe vorgelegen. Gleichwohl hat er die Fotos und Daten gelöscht.

12.2 Beihilfe für Familienmitglieder ohne Kenntnis der oder des Berechtigten

Eine Beratungsstelle hat uns gefragt, wie in Fällen von Beihilfen für Familienangehörige gewährleistet wird, dass die Berechtigten darüber keine Kenntnis erhalten. Es würde als problematisch angesehen, wenn beihilfeberechtigte Eltern durch Vorlage der Abrechnungsbelege über die ärztliche Behandlung oder den Bezug von Medikamenten et cetera beispielsweise ihrer erwachsenen Kinder informiert würden.

Der für die Gewährung der Beihilfe zuständige Eigenbetrieb Performa Nord hat auf unsere Anfrage mitgeteilt, im Fall beihilfeberechtigter erwachsener Kinder bei getrennt lebenden Ehe- oder Lebenspartnern werde auf deren Antrag eine eigene Antragstellung auf Beihilfe gewährleistet. Sonstige Fälle, beispielsweise bei Beihilfeanträgen zu Aufwendungen für Verhütungsmittel oder zu psychotherapeutischen Maßnahmen, seien dort nicht bekannt. Sollten jedoch hierfür entsprechende Gründe vorliegen, bestehe eine gleichgelagerte Antragsmöglichkeit.

12.3 Nennung des Themas eines Bildungsurlaubs auf der Anmelde- und Teilnahmebescheinigung

Die Bescheinigungen zur Teilnahme am Bildungsurlaub enthalten regelmäßig das Thema der Veranstaltung. Von einem Teilnehmer an einem Bildungsurlaub wurde moniert, dass Arbeitgeber durch die ihnen vorzulegenden Dokumente Kenntnis über das Thema erhalten, obwohl diese für die Genehmigung des Bildungsurlaubs nach dem Bremischen Bildungsurlaubsgesetz nicht erforderlich ist. Zudem würden schutzwürdige Interessen der Beschäftigten verletzt, wenn Arbeitgeber Kenntnis

davon erhielten, dass Beschäftigte beispielsweise an Bildungsurlauben mit Themen wie insbesondere Sucht oder sexuelle Identität teilnehmen und dass sie erfahren, welche Themen bevorzugt werden.

Auf unsere Anfrage hin hat die Senatorin für Bildung und Wissenschaft zur Rechtfertigung dieser Praxis auf ein Urteil des Bundesverfassungsgerichts aus dem Jahr 1988 verwiesen, das sich auf die Bundesländer Hessen und Nordrhein-Westfalen bezieht. Danach obliege es den Fachgerichten (zum Beispiel dem Arbeitsgericht) zu erkennen, ob thematisch umstrittene Bildungsveranstaltungen inhaltlich den gesetzlichen Zielvorgaben (berufliche und politische Weiterbildung) entsprechen. Begründet hat das Gericht dies damit, dass es in diesem Bereich vereinzelt zu Rechtsmissbräuchen kommen könne. Nach dem Bremischen Bildungsurlaubsgesetz dient der Bildungsurlaub allerdings nicht nur der politischen und beruflichen, sondern auch der allgemeinen Weiterbildung.

Die verfassungsrechtlich garantierte Möglichkeit für Arbeitgeber, im Zweifelsfall die Übereinstimmung konkreter Bildungsurlaubsveranstaltungen mit den gesetzlichen Zielen gerichtlich überprüfen zu lassen, hat jedoch nicht zur Folge, dass diese bei jedem Bildungsurlaubsantrag Kenntnis über das Thema der Veranstaltung haben dürfen. Vielmehr sind die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit beachtlich. Daher dürfte es angemessen sein, wenn Arbeitgeber lediglich stichprobenartig oder bei tatsächlichen Anhaltspunkten für das Vorliegen eines Rechtsmissbrauchs von der oder dem Beschäftigten Auskunft über das Thema des Bildungsurlaubs verlangen. Daher sollten die Veranstalter von Bildungsurlaubsmaßnahmen in den Anmelde- und Teilnahmebescheinigungen auf die Angabe des Themas und die Veranstaltungsnummer verzichten.

Wir haben die senatorische Dienststelle gebeten, darauf hinzuwirken, dass die Veranstalter ihr Verfahren entsprechend ändern. Nur auf Wunsch einer Teilnehmerin oder eines Teilnehmers sollte das Thema in die entsprechenden Dokumente übernommen werden. Nach unserer Kenntnis verfahren einige Veranstalter in Bremen bereits in dieser Weise, ohne dass es zu Beschwerden von Arbeitgebern gekommen ist.

In einer Besprechung bei der Senatorin für Bildung und Wissenschaft wurde deutlich, dass unsere Rechtsauffassung von dort geteilt wird. Nach Rückfrage in den anderen Bundesländern hat die senatorische Behörde demgegenüber mitgeteilt, es sei unumgänglich, dass die Veranstalter das Thema des Bildungsurlaubs auf den Bescheinigungen angeben. Begründet wird dies damit, dass das Bremische Bildungsurlaubsgesetz keine direkte behördliche Kontrolle der Bildungsurlaube vorsehe. Aus diesem Grund sei es geboten, den Arbeitgebern eine Kontrollmöglichkeit einzuräumen, die sich nicht auf Stichproben beschränken könne, sondern umfassend gestaltet sein müsse.

12.4 Informantenschutz durch Beschluss des Verwaltungsgerichts Bremen bestätigt

Ein Rechtsanwalt, der ein Unternehmen vertritt, hatte von uns Akteneinsicht erhalten, wobei wir die Angaben über den Petenten beziehungsweise Informanten zu dessen Schutz geschwärzt hatten. Die auf vollständige Akteneinsicht gerichtete Klage vor dem Verwaltungsgericht Bremen hatte keinen Erfolg.

Das Gericht hat entschieden, dass Angaben des Petenten nur zum Zwecke der Datenschutzkontrolle gespeichert seien und deshalb gegenüber dem Kläger zu sperren seien. Lediglich dann, wenn von dem Betroffenen berechtigte Interessen an der Kenntnis der erwünschten Daten dargelegt würden, könne eine Akteneinsicht in Betracht kommen. Solche Interessen seien jedoch nicht dargelegt worden. Das Interesse des Klägers bestehe im Kern darin, gegen den Petenten in irgendeiner Weise vorgehen zu können. Da die Aufsichtsbehörde grundsätzlich gehalten sei, von dem Petenten gemachte Angaben vertraulich zu behandeln und damit auch seinen Namen nicht preiszugeben, bedürfe es besonderer Umstände, um dagegen berechtigte Interessen ins Feld zu führen. Das könne bejaht werden, wenn der Petent wider besseren Wissens den Vorwurf von Datenschutzverstößen erhebe oder seine Eingabe strafbare Beleidigungen, üble Nachreden oder eine falsche Anschuldigung enthielten. Dementsprechend bestehe bei Verleumdungen ein berechtigtes Interesse an der Auskunft über den Informanten. Das Urteil ist unter www.datenschutz.bremen.de nachzulesen.

Gegen diesen Beschluss ist Berufung vor dem Oberverwaltungsgericht (OVG) Bremen eingelegt worden. Eine Entscheidung des OVG über die Zulassung der Berufung lag bis zum Redaktionsschluss nicht vor.

Nach unseren Erfahrungen ist der Beschluss des Verwaltungsgerichts Bremen insbesondere im Arbeitsverhältnis beachtlich. Beschäftigte von privatwirtschaftlichen Unternehmen äußern regelmäßig ihre Angst vor der Offenbarung ihrer Identität gegenüber ihren Arbeitgebern, weil sie schwerwiegende Nachteile bis hin zur Entlassung befürchten.

12.5 Schaffung gesetzlicher Regelungen zum Beschäftigtendatenschutz

Im Spätsommer 2010 hat die Bundesregierung dem Bundesrat einen Entwurf zur Änderung des Bundesdatenschutzgesetzes (BDSG) vorgelegt. Dieser soll gegenüber der im Jahr 2009 erfolgten Neuregelung des § 32 BDSG weiter gefasste Regelungen zum Beschäftigtendatenschutz enthalten. Diese Vorschrift war aufgrund der vielen Datenschutzskandale der letzten Jahre in das BDSG eingefügt worden. Der nunmehr vorliegende Entwurf soll nach dem Willen der Bundesregierung umfassende gesetzliche Regelungen für den Arbeitnehmerdatenschutz verwirklichen. Damit soll die Rechtssicherheit für Arbeitgeber und Beschäftigte erhöht werden. Einerseits sollen die Beschäftigten vor unrechtmäßiger Erhebung und Verwendung ihrer Daten geschützt, andererseits sollen die Informationsinteressen der Arbeitgeber beachtet werden.

Der vorgelegte Entwurf entspricht nicht den langjährigen Forderungen, den Beschäftigtendatenschutz in einem eigenen Spezialgesetz zu regeln. Auch wenn der Regierungsentwurf Verbesserungen gegenüber den Vorentwürfen aus dem Frühjahr 2010 enthält, bleibt er weit hinter dem in der arbeitsgerichtlichen Rechtsprechung entwickelten datenschutzrechtlichen Schutzniveau zurück. Zu den Vorentwürfen hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits am 22. Juni 2010 die Entschließung „Beschäftigtendatenschutz stärken statt abbauen“ (vergleiche Ziffer 19.6 dieses Berichts) gefasst.

Im Rahmen der Länderbeteiligung haben wir gegenüber der bremischen Senatskommissarin für den Datenschutz zu dem Regierungsentwurf Stellung genommen. Dabei haben wir insbesondere folgende Änderungsvorschläge angeregt:

— kein Unterlaufen des Schutzstandards des BDSG durch Betriebs- oder Dienstvereinbarungen,

— Fragen nach Vorstrafen und Vermögensverhältnissen nur bei Einsatz in bestimmten Arbeitsbereichen mit finanzieller Verantwortungsbreite,

— keine Frage nach laufenden Ermittlungsverfahren,

— kein Unterlaufen der Direkterhebung durch Datenerhebung in Internetsuchmaschinen und sozialen Netzwerken,

— keine Datenerhebung aufgrund einer nicht wirksamen Einwilligung der Bewerberin oder des Bewerbers,

— Durchführung von Screening-Verfahren nur unter engen Grenzen unter Beachtung des Grundsatzes der Verhältnismäßigkeit und einer angemessenen Abwägung der Rechtsgüter des Arbeitgebers und der oder des Beschäftigten,

— keinen flächendeckenden Verdacht schöpfen,

— Videoüberwachung nur unter Ausschluss von Leistungs- und Verhaltenskontrollen,

— keine unverhältnismäßigen Kontrollen der Telekommunikation und Beachtung des Fernmeldegeheimnisses,

— uneingeschränktes Beschwerderecht der oder des Beschäftigten bei der Aufsichtsbehörde für den Datenschutz ohne vorherige Einschaltung des Arbeitgebers.

Erfreulicherweise hat die Senatskommissarin für den Datenschutz alle unsere Vorschläge in die Beratungen der Ausschüsse des Bundesrats eingebracht. Nicht zuletzt enthält die Stellungnahme des Bundesrats eine Vielzahl der von den Datenschutzbeauftragten der Länder vorgeschlagenen Verbesserungen. Es bleibt zu hoffen, dass das Gesetzgebungsverfahren im Bundestag die vom Bundesrat vorgeschlagenen Verbesserungen berücksichtigt.

13. Auskunfteien

13.1 Eingaben im Bereich der Handels- und Wirtschaftsauskunfteien

Im Berichtsjahr erhielten wir erneut zahlreiche Eingaben von Bürgerinnen und Bürgern, die die Verarbeitung personenbezogener Daten durch Handels- und Wirtschaftsauskunfteien zum Gegenstand hatten. Die Eingaben betrafen unter anderem die Nichterteilung, die nicht vollständige und auch die unrichtige Erteilung von Auskünften an Betroffene. Häufig erst, nachdem wir tätig wurden, war die betreffende Auskunftei bereit, dem Auskunftsanspruch der oder des Betroffenen Rechnung zu tragen.

Zahlreiche Petentinnen und Petenten beklagten sich bei uns, dass eine Auskunftei nicht bereit sei, ihnen auf ihre schriftlichen Auskunftsersuchen mitzuteilen, welche Daten von ihr über sie gespeichert würden. Die Auskunftei begründete die verweigerte Auskunftserteilung mit ihrem Ansinnen, dass vor der Erteilung von Auskünften Kopien der Personalausweise oder Pässe der betreffenden Petenten vorliegen müssten, um eine ausreichende Identifikation des Auskunftsbegehrenden vornehmen zu können.

Ein Anspruch auf die Vorlage einer Kopie des Ausweises, des Passes, auch der Meldebescheinigung, der Auskunftssuchenden mit Angaben zur Person, die über den für die Identifikation benötigten Datenumfang erheblich hinausgehen, besteht für die Auskunftei aber grundsätzlich nicht. Es gibt regelmäßig weitere und je nach Sachlage andere ausreichende Möglichkeiten, eine Auskunft an die hierzu berechtigte Person sicherzustellen. Reichen die von dem oder der Auskunftssuchenden zur Identifikation gemachten Angaben im Einzelfall nicht aus, so kann erforderlichenfalls die Identität zum Beispiel auch mithilfe einer beglaubigten Unterschrift nachgewiesen, die angegebene Anschrift der betroffenen Person anhand allgemein zugänglicher Verzeichnisse, nötigenfalls auch durch Rückgriff auf das Einwohnermelderegister, überprüft werden. Darüber hinaus kann auch die Übersendung der Kopie eines Legitimationsdokuments angesichts der heutigen technischen Möglichkeiten keine hundertprozentige Sicherheit hinsichtlich der Identität der Betroffenen bieten. Es ist mit den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) jedenfalls nicht zu vereinbaren, dass die Erteilung einer Selbstauskunft generell von der Vorlage einer Ausweis- oder Passkopie abhängig gemacht wird.

Wir forderten die Auskunftei auf, die zu beachtenden Vorgaben einzuhalten. Eine Zusage der Auskunftei, dieses zu beachten, steht bislang aber noch aus.

Daneben befassten wir uns unter anderem auch weiterhin mit der Eingabe eines Bürgers, zu dessen Person von einer Auskunftei aufgrund von Anfragen zu dem von ihm geleiteten Unternehmen Auskünfte erteilt worden waren (vergleiche 32. Jahresbericht, Ziffer 13.6.1). Der Anspruch auf Mitteilung, an wen die Daten weitergegeben worden sind, ist umfassend und bezieht sich auf alle Datenübermittlungen. Er beschränkt sich nicht auf die Übermittlungen, bei denen eine Anfrage direkt zu der Person des Betroffenen beauskunftet wird. Die Vertreter der Auskunftei sagten nunmehr zu, dass ihr Unternehmen künftig bis auf Weiteres ohne Anerkennung einer Rechtspflicht der Auffassung der Aufsichtsbehörde Rechnung tragen wird. Unser Petent erhielt daher die von ihm verlangte Auskunft.

Die vorsätzliche oder fahrlässige Nichterteilung von Auskünften an die betroffene Person entgegen den Bestimmungen des § 34 BDSG stellt eine Ordnungswidrigkeit dar, die mit einer Geldbuße bis zu 50.000 Euro geahndet werden kann. Verstöße gegen die Auskunftspflicht nach § 34 BDSG wurden von uns im Berichtsjahr erstmalig als Ordnungswidrigkeit verfolgt (vergleiche Ziffer 17.1 dieses Berichts).

13.2 Einrichtung des Amtes eines Ombudsmanns bei der SCHUFA

Nach dem Vorbild anderer privater Branchen hat die Verbraucherauskunftei SCHUFA im Sommer vergangenen Jahres das Amt eines Ombudsmanns eingerichtet. Dieser Ombudsmann soll als unparteiische, unabhängige Schiedsperson in Streitfällen zwischen Betroffenen und der SCHUFA eine kostenfreie, außergerichtliche Streitbeilegung ermöglichen. Bekleidet wird das Amt derzeit von einem ehemaligen Richter des Bundesverfassungsgerichts. Betroffene erreichen den Ombudsmann postalisch wie folgt: SCHUFA Ombudsmann, Postfach 5280, 65042 Wiesbaden.

14. Videoüberwachung

Videokameras sind mittlerweile in vielen Lebensbereichen allgegenwärtig. Sie erfassen alle Menschen, egal, aus welchem Grund diese sich im Beobachtungs- beziehungsweise Aufzeichnungsbereich aufhalten, gehen, stehen oder fahren. Der Eingriff in das informationelle Selbstbestimmungsrecht beginnt bereits, sobald Einzelpersonen oder Fahrzeuge individuell erkennbar werden. Daher muss eine Videoüberwachung immer auf eine ausdrückliche Rechtsvorschrift gestützt sein. Für die von privaten Stellen eingesetzten Kameras ist dies der § 6 b des Bundesdatenschutzgesetzes. Demgegenüber ist für öffentliche Stellen, die ihre Dienstgebäude und Einrichtungen mit Videokameras ausstatten, der § 20 b des Bremischen Datenschutzgesetzes als gesetzliche Grundlage heranzuziehen. Darüber hinaus gibt es noch Regelungen in speziellen Gesetzen, so etwa für polizeiliche Überwachungsmaßnahmen. Hinsichtlich einer Videoüberwachung im ausschließlich privaten Bereich, wie zum Beispiel im Nachbarschaftsverhältnis, möchten wir in diesem Zusammenhang auf unsere Internetseite www.datenschutz.bremen.de hinweisen. Hier sind eine Orientierungshilfe zur Überwachung mit Videokameras durch nicht öffentliche Stellen sowie ein sehr informatives Gerichtsurteil hinterlegt.

Im öffentlichen wie im privaten, allgemein zugänglichen Bereich gilt, dass ein überwachter Bereich mit eindeutigen Hinweisschildern gekennzeichnet sein muss. Für Passantinnen und Passanten muss erkennbar sein, dass sie sich in einem überwachten Bereich bewegen. Darüber hinaus ist auf dem Hinweis die verantwortliche Stelle mit aufzunehmen. Hierdurch ist es den Betroffenen möglich, ohne weitere Recherchen festzustellen, wer diese Stelle ist, um ihr gegenüber Datenschutzrechte geltend zu machen. Des Weiteren ist die räumliche und zeitliche Ausdehnung der Videoüberwachung auf das für den Zweck erforderliche Maß zu beschränken. Dies ist durch technische und organisatorische Maßnahmen sicherzustellen.

Nachfolgend schildern wir beispielhaft einige Fälle der Videoüberwachung aus verschiedenen Bereichen im Berichtszeitraum.

14.1 Öffentlicher Bereich

14.1.1 Überwachung von Gewahrsamszellen

Wir wurden von der Polizei Bremen um eine Einschätzung zur Zulässigkeit von Videoüberwachungskameras in Gewahrsamszellen gebeten. Hintergrund war der Selbsttötungsversuch einer in Gewahrsam genommenen Person. Die Kameras sollen dem Schutz der festgenommenen Personen dienen. Das gezielte Beobachten von Menschen mit Hilfe von Videotechnik stellt eine Datenerhebung im Sinne des Bremischen Datenschutzgesetzes dar. Voraussetzung für die Zulässigkeit ist daher das Vorliegen einer Einwilligung oder einer Rechtsgrundlage. Eine Einwilligung muss auf der freien Entscheidung der Betroffenen beruhen. Häufig befinden sich in Gewahrsam genommene Personen in einem alkoholisierten Zustand oder einer psychischen Ausnahmesituation. Das Vorliegen einer freien Willensentscheidung steht daher regelmäßig infrage. Wir vertreten deswegen die Auffassung, dass eine Rechtsgrundlage für den Einsatz der Kameras erforderlich ist. Eine ausdrückliche Norm, die die Videoüberwachung von Gewahrsamszellen regelt, enthält das Bremische Polizeigesetz nicht. Die allgemeinen Vorschriften des Gesetzes können nicht als Rechtsgrundlage herangezogen werden, denn Einschränkungen des Rechts auf informationelle Selbstbestimmung bedürfen nach dem Bundesverfassungsgericht einer gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entspricht und verhältnismäßig ist. Die konkreten Anforderungen an die Bestimmtheit und Klarheit der Ermächtigung richten sich nach der Art und Schwere des Eingriffs. Überwachungsmaßnahmen im Gewahrsam stellen einen tiefgreifenden Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen dar. Rückzugsraum vor der Überwachung besteht nicht oder nur in sehr eingeschränktem Maße. Sämtliche Verhaltensweisen, selbst die, die der Intimsphäre zuzuordnen sind, werden registriert. Anders als bei einer unmittelbaren Beobachtung durch eine Mitarbeiterin oder eines Mitarbeiters ohne Kamera weiß die oder der Betroffene nicht, wann sie oder er kontrolliert wird und kann ihr oder sein Verhalten nicht darauf einstellen. Das ständige Gefühl des Beobachtet-Werdens führt zu einem starken Überwachungsdruck. Übersehen werden darf in diesem Zusammenhang allerdings auch nicht das Recht auf Leben und körperliche Unversehrtheit der Betroffenen, dessen Schutz Aufgabe der diensthabenden Polizeibeamten ist. Insofern halten wir eine Videoüberwachung von Gewahrsamszellen nicht für gänzlich un-

zulässig. Erforderlich ist allerdings eine konkrete Rechtsgrundlage. So hat auch das Bundesverfassungsgericht in seiner Entscheidung vom 23. Februar 2007 ausdrücklich festgestellt, dass für die Videoüberwachung öffentlicher Räume eine bereichsspezifische Rechtsgrundlage erforderlich ist. Allgemeine Vorschriften über die Erhebung und Verarbeitung personenbezogener Daten reichen nicht aus. Diese Grundsätze sind auf nicht öffentlich zugängliche Räume übertragbar. Eine Videoüberwachung wiegt dort mindestens genauso schwer wie bei öffentlich zugänglichen Räumen, insbesondere, wenn sich der Betroffene der Überwachung nicht entziehen kann. Voraussetzung für eine Videoüberwachung von Gewahrsamszellen ist daher eine spezielle Rechtsgrundlage im Bremischen Polizeigesetz.

14.1.2 Polizeiliche Videoüberwachung bei Versammlungen

Eine aktuelle Entscheidung des Oberverwaltungsgerichts Münster vom 23. November 2010 betrifft die polizeiliche Videobeobachtung einer friedlichen Versammlung. Die Polizei hatte mittels Kamera-Monitor-Prinzip die Versammlung von etwa 40 bis 70 Personen mit Videokameras beobachtet. Das Kamera-Monitor-Verfahren bedeutet, dass von einer aufnahmebereiten Kamera Bilder in Echtzeit auf einen Monitor in einen voranfahrenden Kamerawagen der Polizei übertragen werden. Das Gericht entschied, dass die konkrete Kameraübertragung einer friedlichen Versammlung durch die Polizei auch ohne die tatsächliche Speicherung der Bilder unzulässig ist. Das Verwaltungsgericht Münster hatte bereits mit Urteil vom 21. August 2009 einen Eingriff in das informationelle Selbstbestimmungsrecht neben einem Eingriff in das Grundrecht auf Versammlungsfreiheit festgestellt. Mit einem ähnlich gelagerten Fall beschäftigte sich das Verwaltungsgericht Berlin mit Urteil vom 5. Juli 2010 und nahm eine Grundrechtsverletzung des informationellen Selbstbestimmungsrechts an. Wir gehen davon aus, dass die Landespolizeien die in diesen verwaltungsrechtlichen Entscheidungen aufgestellten Grundsätze beachten.

14.1.3 Videoüberwachung der Kassenautomaten

Bei einem anderweitigen Termin im Sozialzentrum Gröpelingen/Walle sind wir darauf aufmerksam geworden, dass der im Gebäude aufgestellte Kassenautomat videoüberwacht wird und kein Hinweisschild auf die Überwachung vorhanden war. Weiter stellten wir fest, dass zwei Kameras installiert waren, wobei sich eine Kamera an der Wand gegenüber dem Geldautomaten befand und die andere im Geldautomaten selbst eingebaut war. Aufgrund unserer Anfrage teilte das Amt für Soziale Dienste mit, die Videoüberwachung diene dem Schutz der Personen, die Geld aus dem Automaten entnähmen. Ferner solle im Streitfall nachgewiesen werden, dass überhaupt Geld ausgezahlt worden sei, falls eine Person Gegenteiliges behaupte. Wir haben erreicht, dass die Dienstanweisung des Amtes für Soziale Dienste zur Videoüberwachung nunmehr den Vorgaben des Bremischen Datenschutzgesetzes entspricht. Sie enthält jetzt auch Angaben über den Überwachungsbereich sowie die aktuellen Löschfristen der Videoaufzeichnungen. Darüber hinaus wurde uns bestätigt, dass deutlich sichtbare Hinweisschilder angebracht werden, die auf den Umstand der Videoüberwachung hinweisen.

14.2 Nicht öffentlicher Bereich

14.2.1 Videoüberwachung der Bürgerweide

Im Berichtszeitraum wurde uns vom Petitionsausschuss der Bremischen Bürgerschaft eine Petition zur Videoüberwachung der Bürgerweide mit der Bitte um Stellungnahme übersandt. In der Beschwerde wurde kritisiert, dass alle Menschen beim Überqueren der Bürgerweide von Videokameras überwacht würden und dies auch bei dort stattfindenden Veranstaltungen der Fall sein könnte. Die Kameras seien schwenkbar und hätten eine Zoomfunktion. Ebenso seien keine ausreichenden Hinweisschilder vorhanden. Daraufhin haben wir bei der für die Videoüberwachung verantwortlichen Stelle eine Prüfung der Überwachungsanlage durchgeführt. Es wurde uns bestätigt, dass nur die beiden deutlich durch rot-weiße Begrenzungspoller gekennzeichneten Parkbereiche überwacht werden sollen. Die Anlage dient dem Zweck, einen möglichst reibungslosen, kundenorientierten Parkverkehr zu gewährleisten. Die Kunden hätten bei Problemen mit der Parkordnung die Möglichkeit, die Leitzentrale per Ruftaste um Hilfestellung zu bitten, wenn zum Beispiel die Zuwegungen durch Falschparker blockiert würden, es zu Problemen bei der Schrankentechnik der Zufahrten und Ausfahrten komme oder Fahrzeuge zugeparkt

würden. Nur in diesen Fällen schaltet sich die Leitzentrale auf die entsprechende Kamera auf und schwenkt auf den betroffenen Bereich. Eine permanente Überwachung der Parkbereiche findet somit nicht statt.

Im Rahmen der Prüfung wurden die genauen Schwenkbereiche der Kameras festgelegt, sodass künftig tatsächlich nur noch die Parkflächen erfasst werden. Bereiche außerhalb der Parkzonen (Spielplatz, öffentliche Straßen, Zugang zur Stadthalle in Höhe der Klangbögen) können somit von den Kameras nicht erfasst werden.

Darüber hinaus haben wir erreicht, dass an den Masten im Randbereich der Parkzonen zusätzliche Hinweisschilder angebracht werden. Somit werden Passantinnen und Passanten, die die Bürgerweide über die Parkflächen queren, über die Videoüberwachung informiert. Da bei Großveranstaltungen keine Videoüberwachung durchgeführt wird, wurde uns von der verantwortlichen Stelle zugesichert, dass auch auf diesen Umstand durch zusätzliche Schilder an den Masten der Kameras hingewiesen wird. Ferner wurde von der verantwortlichen Stelle die Verfahrensbeschreibung zeitnah ergänzt, die von jedermann eingesehen werden kann. Das Ergebnis wurde sowohl dem Petitionsausschuss als auch dem Beschwerdeführer mitgeteilt.

14.2.2 Videoüberwachung des öffentlichen Bereiches durch eine an der Hauswand installierte Kamera

Im Mai 2010 wurden wir darauf hingewiesen, dass an der Hauswand eines Restaurants über der Eingangstür eine Videokamera installiert sei. Durch die Ausrichtung der Kamera sei zu befürchten, dass der komplette öffentliche Gehweg sowie die Straße überwacht würden.

Auf unsere Anfrage hin teilte der Mieter des Restaurants mit, dass er zwei Kameras an der Fassade installiert habe, die rund um die Uhr aufzeichneten. Die Installation sei erforderlich gewesen, weil die Schaufenster zuvor beschädigt worden seien und die mit Granit verkleidete Fassade mit Graffiti besprüht worden sei. Darüber hinaus sei noch eine Kamera im Innenbereich des Restaurants installiert worden sowie ein Bildschirm zur Kontrolle des laufenden Bildes dieser Kamera. Daraufhin haben wir den Restaurantbesitzer die rechtlichen Voraussetzungen zur Videoüberwachung eingehend geschildert. Außerdem teilten wir ihm mit, welche Maßnahmen von ihm umzusetzen sind, damit die Überwachung den gesetzlichen Anforderungen an den Datenschutz gerecht wird. Abschließend bestätigte uns der Restaurantbesitzer, dass er die Kamera im Innenbereich sowie den Bildschirm abmontiert hätte. Gleichzeitig seien die zwei Kameras an der Fassade so ausgerichtet worden, dass sie nur den unmittelbaren Fassadenbereich sowie die Schaufenster erfassten und sie würden nur bei Dunkelheit außerhalb der Geschäftszeiten aktiviert. Ebenso habe er an der Hausfront deutlich sichtbare Hinweisschilder angebracht, die auf die Überwachung hinweisen. Außerdem wurde die von uns geforderte und für jedermann einsehbare Verfahrensbeschreibung zur Videoüberwachung erstellt.

14.2.3 Videoüberwachung in Taxen

Im September 2010 wurden wir von einem Fahrgast darüber unterrichtet, dass er bei einer Fahrt in einem Taxi von einer Videokamera überwacht worden sei. Auf seine Nachfrage beim Taxifahrer habe dieser ihm bestätigt, dass die Videokamera permanent laufe und auch die im Taxi geführten Gespräche aufgezeichnet würden. Darüber hinaus sei der Fahrgast weder vor Beginn der Fahrt in irgendeiner Weise auf die Aufnahmen aufmerksam gemacht worden, noch sei das Taxi entsprechend gekennzeichnet gewesen. Der zur Rede gestellte Taxifahrer habe überdies abgelehnt, die Aufnahmen zu beenden, da er keinen Einfluss auf diese habe.

Mit der betroffenen Taxizentrale haben wir bereits im Sommer 2010 die Änderungen hinsichtlich der Videoüberwachung in Taxen abgesprochen. Wir haben daher diese Eingabe zum Anlass genommen, die Umsetzung der abgesprochenen Maßnahmen zu kontrollieren und eine Prüfung der Videoüberwachungsanlage in der Taxizentrale vorzunehmen. Hierbei wurde von uns das fragliche Taxi in Augenschein genommen und weitere Taxen stichprobenartig überprüft.

Es wurde festgestellt, dass die getroffenen technischen und organisatorischen Maßnahmen den datenschutzrechtlichen Anforderungen gerecht werden und die von

uns insoweit geforderten Maßnahmen umgesetzt wurden. Es findet keine permanente Aufzeichnung der Videobilder, sondern nur eine periodische Standbildaufnahme statt. Ebenso werden die Gespräche in den Taxen, mit Ausnahme von Notfallsituationen, grundsätzlich nicht aufgenommen.

Weiterhin konnten wir bei der Inaugenscheinnahme der Taxen feststellen, dass durch Aufkleber auf die Videoüberwachung hingewiesen wird. Die Hinweise befanden sich an den Scheiben der Beifahrertür sowie den Fondtüren.

Die Taxizentrale hat ein Merkblatt erstellt, das künftig in jedem Taxi ausgelegt wird. Aus diesem geht hervor, dass nur einzelne Bilder aufgezeichnet werden und ein Mithören von Gesprächen im Taxi nur in Notfallsituationen möglich ist. Ziel ist, dass die Fahrgäste, aber auch die Fahrerinnen und Fahrer selbst, korrekt informiert sind und Letztere keine falschen Auskünfte geben können. Darüber findet sich in dem Merkblatt ein Hinweis, wonach bei Bedarf die komplette Verfahrensbeschreibung des Systems bei der Zentrale oder im Internet eingesehen werden kann.

15. Dienstleistungen, Handel und Werbung

15.1 Missachtung datenschutzrechtlicher Rechtspositionen durch Internetdienstleister

Eine Vielzahl von bei uns eingegangener Beschwerden aus dem gesamten Bundesgebiet betrafen und betreffen ein Unternehmen, das als Premium Software GmbH firmiert und ursprünglich als Unternehmenssitz eine Bremerhavener Adresse führte. Auf seiner Internetseite www.abcload.de beziehungsweise www.premsw.de unter „Produkte“ bot das Unternehmen Software zum Download (Herunterladen) an, insbesondere auch sogenannte Freeware, also kostenfrei im Internet angebotene Software unterschiedlicher Hersteller. Nutzerinnen und Nutzer des Angebots wurden jedoch nach Herunterladen der jeweiligen Freeware zu ihrer Überraschung alsbald seitens des Unternehmens via E-Mail zur Zahlung eines Betrages aufgefordert. Zur Begründung seiner Zahlungsaufforderung führte das Unternehmen an, die Nutzerin oder der Nutzer habe ein entgeltliches Abonnement mit einjähriger Mindestlaufzeit abgeschlossen. Bei Nichtzahlung wurden Nutzerinnen beziehungsweise Nutzer mit aggressiven Mahnungen zur Zahlung gedrängt. Aufgrund dieser Geschäftspraktik nahm die Verbraucherzentrale Hamburg das Unternehmen mit der vorstehend genannten Internetseite auf eine umfangreiche Liste von Unternehmen auf, die in den Verdacht des Betriebs einer sogenannten „Internet-Abofalle“ geraten sind.

Obwohl die Geschäftspraktik des Unternehmens in erster Linie zivilrechtliche sowie strafrechtliche Fragen aufwirft, beschäftigte und beschäftigt das Unternehmen auch uns als Datenschutzaufsichtsbehörde. Viele der Betroffenen wandten sich nämlich an uns, weil sie von dem Unternehmen eine Löschung ihrer Daten oder eine Eigenauskunft über die seitens des Unternehmens gespeicherten personenbezogenen Daten gefordert hatten, das Unternehmen entgegen seiner gesetzlichen Pflichten jedoch nicht reagierte. Auf unser Tätigwerden zur Durchsetzung der Betroffenenrechte hin mussten wir feststellen, dass unter der Geschäftsanschrift in Bremerhaven weder ein Geschäftslokal noch ein Briefkasten existierte. Die auf den via E-Mail versandten Zahlungsaufforderungen angegebene Telefonnummer existierte nicht und über das elektronische Kontaktformular konnte kein Kontakt hergestellt werden. Auch der Geschäftsführer des Unternehmens entzog sich Kontaktaufnahmeversuchen; eine Privatanschrift war nicht ermittelbar. Wir werden gleichwohl weiterhin nichts unversucht lassen, das Datenschutzrecht mit allen uns zur Verfügung stehenden Mitteln gegenüber dem Unternehmen einschließlich seiner Geschäftsführung durchzusetzen und begangene Verstöße zu ahnden. Betroffenen, die Zahlungsaufforderungen der Premium Software GmbH erhalten haben oder noch erhalten, sei vor einer Zahlung empfohlen, rechtlichen Rat einzuholen. Als Ansprechpartnerinnen stehen – soweit es nicht um datenschutzrechtliche Betroffenenrechte geht – insbesondere die Verbraucherzentralen zur Verfügung. Gegebenenfalls sollten sich Betroffene auch mit der Staatsanwaltschaft in Verbindung setzen.

15.2 Telefonanrufe angeblicher Datenschutzeinrichtungen

Wie auch die Aufsichtsbehörden anderer Länder erhielten wir im Berichtszeitraum durch Nachfragen betroffener Bürgerinnen und Bürger Kenntnis davon, dass es, ähnlich wie im Vorjahr, wieder zahlreiche Versuche gab, die im Zuge der Daten-

schutzskandale aufgekommenen Sorgen vor einem Missbrauch persönlicher Daten zu unlauteren Zwecken auszunutzen. Opfer der unlauteren Geschäftspraktiken waren beziehungsweise sind zumeist ältere Personen, die gezielt etwa anhand der Art des Vornamens oder auch aufgrund der Kenntnis des Geburtsdatums als Ansprechpartnerinnen beziehungsweise Ansprechpartner ausgewählt werden.

In den uns bekannt gewordenen Fällen meldeten sich via Telefonanruf angebliche Mitarbeiterinnen oder Mitarbeiter einer vermeintlichen Datenschutzeinrichtung, die etwa als Amt für Datenschutz, als Datensperrdienst, Bundesdatenschutzamt oder unter ähnlicher Bezeichnung vorgestellt wurde. Im Gespräch wurde sodann zum Beispiel mitgeteilt, dass man festgestellt habe, dass sich Daten der oder des Angerufenen „im Umlauf" befänden. Gegen ein geringes monatliches oder einmaliges Entgelt würde man dafür Sorge tragen, dass diese Daten gesperrt beziehungsweise gelöscht würden. Von der Annahme solcher Offerten kann nur eindringlich abgeraten werden. Sollte unter Bezugnahme auf ein derartiges Telefonat ein Vertragsabschluss behauptet und eine Zahlung eingefordert werden, so empfiehlt es sich, vor der Zahlung zunächst rechtlichen Rat, etwa bei den Verbraucherzentralen, einzuholen. Handelt es sich, wie hier, zugleich um telefonische Werbung für eine Leistung, in deren Erbringung seitens der oder des Angerufenen nicht zuvor ausdrücklich eingewilligt wurde, so liegt ein Verstoß gegen das Gesetz gegen den unlauteren Wettbewerb vor. Derartige Gesetzesverstöße können seitens der Bundesnetzagentur verfolgt und geahndet werden.

In einigen Fällen werden den Angerufenen wohl auch – aus welchen Quellen auch immer bezogen – persönliche Daten, namentlich auch Bankverbindungsdaten genannt und im Anschluss nachgefragt, ob diese Daten richtig seien. Auf diese Weise wird unter Ausnutzung des Überraschungseffekts insbesondere versucht, an zutreffende Bankverbindungsdaten zu gelangen, um diese für Abbuchungen zulasten der Betroffenen nutzen zu können. Da keine der staatlichen Datenschutzaufsichtsbehörden oder der Verbraucherschutzinstitutionen auf diese Weise an Betroffene herantreten würde, sollte man sich inhaltlich auf solche Anrufe keinesfalls einlassen, vor allem keine persönlichen Daten nennen oder Fragen hierzu beantworten. Spätestens nach einem solchen Anruf sollten regelmäßig in kurzen Abständen die Kontoauszüge überprüft werden. Wird hierbei dann tatsächlich eine unberechtigte Abbuchung festgestellt, sollte der Lastschrift bei dem kontoführenden Kreditinstitut umgehend widersprochen und gegebenenfalls die Staatsanwaltschaft eingeschaltet werden.

15.3 Einsehbare PIN-Eingabe im Supermarkt

Wir erhielten den Hinweis, im Kassenbereich eines Supermarkts seien an der Decke Spiegel in der Weise angebracht, dass es nachfolgenden Kundinnen und Kunden in der Warteschlange an der Kasse möglich ist, bei einer Bezahlung mit EC-Karte die Eingabe der PIN (Persönliche Identifikationsnummer) durch den gerade bezahlenden Kunden zu beobachten. Weiterhin seien Videokameras im Markt installiert, unter anderem auch derart, dass die Spiegel im Kassenbereich im Erfassungsbereich der Kameras lägen, womit letztlich auch die PIN-Eingaben durch Kundinnen und Kunden aufgezeichnet würden.

Hinsichtlich der Überwachung des Kassenbereichs musste in diesem Fall außerdem geklärt werden, ob die Beschäftigten an der Kasse von der Kamera mit erfasst werden. In diesem Fall würden die Beschäftigten dauerhaft, lückenlos und verdachtsunabhängig videoüberwacht. Dies käme einem Generalverdacht gleich, der einen rechtswidrigen Eingriff in ihr Persönlichkeitsrecht darstellen würde, weil sie insoweit einem unzumutbaren Überwachungsdruck ausgesetzt wären.

Letztlich bestätigte uns der Inhaber, dass die Spiegel im Kassenbereich neu eingestellt worden seien und nunmehr keine Einsichtnahme durch nachfolgende Kundinnen und Kunden erfolgen könne. Ebenso wurden die Kameras im Kassenbereich so ausgerichtet, dass die Spiegel nicht mehr in ihren Erfassungsbereich fallen und auch keine Beschäftigten an der Kasse erfasst werden können. Außerdem wurde eine allgemein einsehbare Verfahrensbeschreibung erstellt.

15.4 Werbung

Auch in diesem Jahr beschäftigte uns aufgrund etlicher Eingaben wieder das Thema Werbung in seinen datenschutzrechtlichen Bezügen.

In jüngerer Zeit gab es einige gesetzgeberische Initiativen im Hinblick auf die Zulässigkeit von Werbung, um erkannte Regelungslücken zu schließen beziehungsweise für mehr Rechtsklarheit zu sorgen. So wurde im Gesetz gegen den unlauteren Wettbewerb geregelt, dass telefonische Werbung gegenüber Verbraucherinnen und Verbrauchern nur dann zulässig ist, wenn diese zuvor hierin ausdrücklich eingewilligt haben. Verstöße hiergegen stellen nunmehr eine Ordnungswidrigkeit dar und können seitens der Bundesnetzagentur verfolgt und durch Geldbuße geahndet werden. In diesem Zusammenhang wurde auch die in der Praxis häufige Rufnummernunterdrückung bei Werbeanrufen durch eine Neuregelung im Telekommunikationsgesetz verboten. Auch im Bundesdatenschutzgesetz (BDSG) wurde die Vorschrift, die die Verwendung personenbezogener Daten zu Werbezwecken regelt, inhaltlich neu gestaltet. Die Neuregelung trägt jedoch weniger datenschutzrechtlichen Belangen als vielmehr Werbeinteressen der Wirtschaft Rechnung und ist zudem in ihrer Formulierung missglückt, was die Kontrolle der Umsetzung durch uns weiter erschwert. Positiv zu bewerten ist die Einfügung neuer Bußgeldtatbestände, die im Bereich von Verstößen gegen werbebezogene Datenschutzregeln nunmehr Sanktionen erlauben.

Gleich mehrere Betroffene suchten unsere Hilfe gegen Spam-Mails eines angeblich in Bremen ansässigen Einzelkaufmanns, der mit Reiseangeboten und Versandhandelsartikeln warb. Diese Werbemaßnahme via E-Mail verstieß bereits ohne Weiteres gegen das Gesetz gegen den unlauteren Wettbewerb. Die Betroffenen hatten nach Erhalt der E-Mail der Nutzung ihrer Daten zu Werbezwecken ausdrücklich widersprochen. Die weitere Nutzung der personenbezogenen Daten zu Werbezwecken wurde hiermit nach dem BDSG unzulässig. Die Weiterverwendung der Daten stellt dann eine Ordnungswidrigkeit dar, die durch uns als Aufsichtsbehörde im äußersten Fall sogar mit einer Geldbuße bis zur Höhe von 300 000 Euro geahndet werden könnte. Daneben hatten die Betroffenen zumeist ihren datenschutzrechtlichen Auskunftsanspruch hinsichtlich der bei dem Absender zu ihrer Person gespeicherten Daten sowie zur Herkunft dieser Daten geltend gemacht. Der vermeintliche Einzelkaufmann „reagierte“ hierauf jedoch lediglich durch Zusendung weiterer Werbe-Mails. Unsere Versuche, den Betroffenen zu ihrem Recht zu verhelfen und gegebenenfalls die Eigenauskunftsverweigerung sowie die Zuwiderhandlung gegen den Werbewiderspruch durch den Mail-Absender im Wege eines Bußgeldverfahrens zu ahnden, blieben im Ergebnis mangels Ermittelbarkeit des Absenders beziehungsweise seines Aufenthaltsorts fürs Erste ohne Erfolg. Den Betroffenen blieb insoweit zunächst nur die Möglichkeit, durch entsprechende Einstellung des Spam-Filters ihres E-Mail-Postfachs die Werbe-Mails auszufiltern.

In einem weiteren Fall der Zusendung einer Werbe-Mail trotz eines vorherigen Werbewiderspruchs des E-Mail-Empfängers handelte es sich nach unseren Erkenntnissen um einen einmaligen, individuellen Fehler einer Mitarbeiterin eines seitens des werbenden Unternehmens zwischengeschalteten Dienstleisters, nicht jedoch um einen systematischen Umsetzungsfehler. Das Unternehmen reagierte auf unser Tätigwerden hin sofort und sperrte die Angaben des Betroffenen für Werbezwecke. Wir sahen hier keinen weiteren Handlungsbedarf.

In einem anderen Beschwerdefall stellte sich heraus, dass die zweite postalische Werbeaktion eines Unternehmens aufgrund ihres Ausmaßes zeitlich bereits weit vor dem Zugang des Werbewiderspruchs des Betroffenen bei einem eingeschalteten spezialisierten Werbedienstleister seitens des Unternehmens in Auftrag gegeben worden war. Die Zusendung des zweiten Werbeschreibens konnte aufgrund des fortgeschrittenen Stadiums nicht mehr rechtzeitig unterbunden werden, was zur Folge hatte, dass der Betroffene wenige Tage nach Absendung seines Werbewiderspruchs erneut Werbepost erhielt und hierüber nachvollziehbarer Weise erbost war. Nachdem wir die Zusammenhänge aufgeklärt und zugleich festgestellt hatten, dass die Betroffenendaten seitens des Unternehmens zeitnah nach Eingang des Werbewiderspruchs gesperrt worden waren, sahen wir auch hier keinen weiteren Handlungsbedarf. Auch der Betroffene war insoweit beruhigt.

Bei einem Teil der bei uns eingegangenen Beschwerden über postalische Werbung stießen wir bei dem Versuch der Durchsetzung der Rechte der Betroffenen erneut auf die Schwierigkeit, dass es sich bei den Werbenden lediglich um sogenannte Postfach-Firmen handelte. Weder das angebliche Unternehmen selbst noch die dahinterstehenden Personen waren mit den uns zur Verfügung stehenden rechtlichen Möglichkeiten ermittelbar (vergleiche 32. Jahresbericht, Ziffer 13.8.3).

In einem weiteren Fall mussten wir erneut feststellen, dass es scheinbar noch nicht allgemein bekannt ist, dass das BDSG bei Werbemaßnahmen eine Informationspflicht des Werbenden gegenüber dem Beworbenen bei der Werbeansprache festschreibt. Nach der entsprechenden Regelung sind die Beworbenen nämlich stets auf die Identität (Name, Kontaktdaten) der werbenden, für die Datennutzung verantwortlichen Stelle sowie auf das Werbewiderspruchsrecht hinzuweisen. Soweit die Durchführung der Werbeaktion durch einen externen Dienstleister ausgeführt wird, der auf eigenes Adressmaterial zurückgreift, muss die werbende Stelle in ihrer Werbeinformation zusätzlich auf diesen Dienstleister als Datenquelle hinweisen, damit die Betroffenen die Herkunft ihrer Daten nachvollziehen und gegebenenfalls die Rechtmäßigkeit der Verwendung überprüfen können. Auch das Unterlassen dieses Hinweises ist mittlerweile als Ordnungswidrigkeitstatbestand ausgestaltet, kann also gegebenenfalls mit einer Geldbuße belegt werden. Auch in diesem Fall reichte jedoch ein Hinweis unsererseits auf die Rechtslage, um unmittelbar entsprechende Veränderungen bei dem Werbenden zu veranlassen.

16. Kreditwirtschaft

Neben anderen Wirtschaftszweigen, wie beispielsweise der Auskunfteienbranche, dem Versicherungsgewerbe und der Werbewirtschaft, ist auch die Kreditwirtschaft ein Sektor, der stets erhöhter Aufmerksamkeit der Datenschutzaufsichtsbehörden bedarf. Kreditinstitute erheben und verwenden in erheblichem Umfang personenbezogene Daten und sind hierzu auch in einer Mehrzahl spezieller Gesetze ausdrücklich ermächtigt. Tendenziell neigen Kreditinstitute dazu, ihre gesetzlichen Erhebungs- und Verwendungsbefugnisse weitestmöglich zu interpretieren. Die bei Datenerhebungen grundsätzlich gebotene Zurückhaltung (Grundsatz der Datenvermeidung und Datensparsamkeit) und die notwendige Sensibilität im Umgang mit den erhobenen Daten ist dabei jedoch leider nicht immer im wünschenswerten Umfang gegeben, was auszugsweise auch an zweien der nachfolgenden Beispiele deutlich wird.

16.1 Datenschutzvorkehrungen bei Selbstbedienungsterminals der Kreditinstitute

Bereits in unserem vorangegangenen Jahresbericht (siehe 32. Jahresbericht, Ziffer 13.9.1.) hatten wir über die mangelhafte Absicherung der eingesetzten Zahlungsverkehrs- beziehungsweise Überweisungsterminals gegen unbefugtes Mitlesen in Filialen der Sparkassen Bremerhaven und Bremen berichtet, welche wir bei einer stichprobenweisen Überprüfung festgestellt hatten. Seitens der Hersteller verfügen die eingesetzten Geräte nicht über einen baulichen Seitensichtschutz am Monitor in Form eines Rahmens oder ähnlicher Bauteile, sodass der Einsatz dieses Gerätetyps trotz einer vorhandenen technischen Sicherungsmaßnahme bei der gegenwärtig offeneren Gestaltung von Filialräumlichkeiten nahezu zwangsläufig zu datenschutzrechtlich nicht hinnehmbaren Situationen führt. Da nach dem Bundesdatenschutzgesetz jede verantwortliche Stelle verpflichtet ist, bei einer automatisierten Datenverarbeitung datenschutzrechtlichen Anforderungen genügende technische und organisatorische Schutzvorkehrungen zu treffen, insbesondere also auch einen wirksamen Schutz gegen unbefugte Einsichtnahme in personenbezogene Daten zu treffen (Zugriffskontrolle), hatten wir diesen Missstand bei den betroffenen Kreditinstituten beanstandet und sie zur Beseitigung des datenschutzrechtswidrigen Zustands aufgefordert. Mit welchen Mitteln ein angemessenes Schutzniveau hergestellt wird, blieb der Entscheidung der Kreditinstitute überlassen.

Nach Prüfung der Abhilfemöglichkeiten entschieden sich die betroffenen Kreditinstitute neben einer Neumarkierung von Diskretionsabständen zu technischen Umstellungen, um die Mitlesbarkeit der Schriftbildanzeige zu reduzieren. Da diese Maßnahmen allein aber in einem Großteil der Filialen nicht ausreichten, um ein hinreichendes Schutzniveau herzustellen, wurden zum Teil Geräte umplatziert oder alternativ nach baulichen Lösungen gesucht.

In einigen Filialen der Sparkasse Bremerhaven nahmen wir die getroffenen Abhilfemaßnahmen in Augenschein. Hier sind unserer Auffassung nach nunmehr hinreichende Schutzvorkehrungen getroffen worden. Die Sparkasse Bremen hatte im Berichtszeitpunkt in einigen wenigen Filialen und Zahlungspunkten bereits zusätzlich bauliche Maßnahmen ergriffen, zum Teil auch schon abgeschlossen, zum Teil erst geplant. Wir nahmen in einer der betroffenen Filialen die bereits abgeschlossenen baulichen Maßnahmen in Augenschein. Auch hier ist unserer Einschätzung nach eine gute Lösung gefunden worden, die datenschutzrechtlichen Gestaltungs-

anforderungen in hinreichender Weise Rechnung trägt. Allerdings besteht in etlichen weiteren Filialen Handlungsbedarf. Angesichts der mittlerweile vergangenen Zeit gehen wir von einer nunmehr zügigen Abhilfe in den übrigen betroffenen Filialen aus. Wir werden die weitere Umsetzung der Abhilfemaßnahmen beobachten.

16.2 Fehlerhafte Erteilung einer geforderten Eigenauskunft an einen Betroffenen

Im Rahmen einer Auseinandersetzung eines Kunden mit seinem Kreditinstitut um die Zulässigkeit einer Datenerhebung durch das Kreditinstitut forderte der betroffene Kunde die Erteilung einer Eigenauskunft über seine bei dem Kreditinstitut gespeicherten personenbezogenen Daten. Das Kreditinstitut kam dieser Aufforderung zunächst nicht nach. Nachdem wir durch den Betroffenen hierüber informiert und um Unterstützung gebeten worden waren, traten wir an das Kreditinstitut heran und wiesen nachdrücklich auf die gesetzliche Auskunftspflicht und den entsprechenden Ordnungswidrigkeitstatbestand, der entsprechende Verstöße sanktioniert, hin. Hierauf erteilte das Kreditinstitut dem Betroffenen eine Auskunft und teilte uns dies mit. Nachdem uns der über die Art der erhaltenen Auskunft höchst überraschte Betroffene die Eigenauskunft vorgelegt hatte, mussten wir feststellen, dass dem Betroffenen lediglich Datenarten (wie die Erfassung der Angaben zur Anschrift), nicht jedoch die konkret gespeicherten, individuellen Daten als solche (der Name der Straße und die Hausnummer) mitgeteilt worden waren. Im Wege des Auskunftsanspruchs soll der Betroffene jedoch unter anderem gerade in die Lage versetzt werden, zu überprüfen, ob die tatsächlich gespeicherten Daten auch der Richtigkeit entsprechen. Daher darf sich die Eigenauskunft niemals lediglich auf die Benennung von Datenarten oder Datenkategorien beschränken. Sie ist im Unterschied zur Datenspeicherungs- beziehungsweise Datenübermittlungsbenachrichtigung immer konkret zu fassen, und zwar hinsichtlich sämtlicher individuell vorhandenen Daten. Wir wandten uns also erneut an das Kreditinstitut und forderten es nochmals zur Auskunftserteilung, diesmal in ordnungsgemäßer Form, auf. Dem wurde fristgerecht Rechnung getragen. Gleichzeitig sicherte das Kreditinstitut uns zu, künftig korrekte Eigenauskünfte zu erteilen.

16.3 Personalausweiskopien bei Kreditinstituten

Mehrere besorgte Bürgerinnen und Bürger wandten sich im Berichtszeitraum wieder mit der Frage an uns, ob es zulässig sei, dass Kreditinstitute anlässlich von Bankgeschäften Kontrollen der Identität anhand von Ausweisdokumenten durchführten und sodann Kopien der vorgelegten Ausweisdokumente anfertigten.

Eine Antwort auf diese Frage gibt das sogenannte Geldwäschegesetz (GwG), dessen Regelungen zum Teil durch weitere bankenrechtliche Gesetze ergänzt oder modifiziert werden. Das Geldwäschegesetz soll, wie es der Gesetzesname bereits sagt, Geldwäsche-Straftaten und Terrorismusfinanzierung verhindern helfen. Kreditinstituten sind daher durch das GwG bestimmte Sorgfaltspflichten auferlegt worden. Zu diesen Sorgfaltspflichten gehört auch in bestimmten Fällen die Identifikation von Vertragspartnern. Identifikation bedeutet nach der gesetzlichen Definition zunächst die Feststellung der Identität durch Erhebung bestimmter Personenangaben und nachfolgend in einem zweiten Schritt die Überprüfung dieser erhobenen Angaben. Zur Feststellung der Identität dürfen bei natürlichen Personen (ausschließlich) die Daten Name, Geburtsort, Geburtsdatum, Staatsangehörigkeit und Anschrift erhoben werden. Die Richtigkeit dieser erhobenen Daten ist dann anhand eines gültigen amtlichen Ausweises gegenzuprüfen.

Diese aufgrund der Sorgfaltspflicht erhobenen Daten über Vertragspartner sind nach dem GwG aufzuzeichnen und für mindestens 5 Jahre aufzubewahren. Zusätzlich zu diesen Daten müssen die Kreditinstitute die Art, die Nummer und die ausstellende Behörde des zur Überprüfung vorgelegten amtlichen Ausweises erfassen. Die Anfertigung einer Kopie des vorgelegten Identifikationsdokuments gilt nach einer ausdrücklichen Regelung des GwG als Aufzeichnung der darin enthaltenen Daten.

Das GwG trifft also exakte Festlegungen hinsichtlich der im Einzelnen zu erhebenden und aufzuzeichnenden Daten bei natürlichen Personen als Vertragspartner. Über diese Daten hinaus enthält beispielsweise der Personalausweis jedoch noch weitere personenbezogene Daten, nämlich Lichtbild, Gültigkeit, eigenhändige Unterschrift, Größe, Augenfarbe, gegebenenfalls Künstlername, Ausstellungsdatum. Zur Erhebung dieser Daten sind die Kreditinstitute nach dem GwG nicht befugt.

Die gesetzlich eingeräumte Möglichkeit, eine Kopie anfertigen zu können anstelle individuelle Eintragungen vornehmen zu müssen, dient einzig und allein der Arbeitserleichterung der Kreditinstitute. Sie erweitert aber nicht deren Datenerhebungsbefugnisse. Zudem sind diese weiteren Personalausweisdaten zu einer Identifizierung nicht erforderlich; Datenerhebungen haben sich jedoch stets am Grundsatz der Erforderlichkeit auszurichten. Hinzu tritt in diesem Zusammenhang noch das im Bundesdatenschutzgesetz (BDSG) verankerte, allgemeinem Geltungsanspruch erhebende Gebot weitestmöglicher Datenvermeidung. Wird also die von Gesetzes wegen vorgesehene „Arbeitserleichterung" Kopie genutzt, so ist seitens der Kreditinstitute darauf zu achten, dass auf diesem Weg nicht der gesetzlich vorgegebene Rahmen der zu erhebenden Daten überschritten wird. Dies kann etwa dadurch geschehen, dass die Daten des vorgelegten Personalausweises, die nicht im Rahmen des Geldwäschegesetzes erhoben werden dürfen, durch Schwärzung unkenntlich gemacht werden.

Hält sich ein Kreditinstitut nicht an diese Beschränkungen, so steht eine unbefugte Datenerhebung und damit gegebenenfalls eine bußgeldbewehrte Ordnungswidrigkeit im Raum. Dem Betroffenen stehen Löschungsansprüche gegenüber dem Kreditinstitut hinsichtlich der überschießend erhobenen Daten zu.

Aufgrund einer Beschwerde überprüften wir im Berichtszeitraum die Identifikationsmaßnahme und nachfolgende Aufzeichnung der erhobenen Daten durch einen Zahlungsdienstleister und mussten dabei feststellen, dass nicht nur die nach dem GwG zugelassenen, sondern vielmehr sämtliche Personalausweisdaten im Wege der Kopie aufgezeichnet worden waren. Nachdem wir dies moniert hatten, wurden die unzulässigerweise erhobenen Daten nach Zusicherung des Zahlungsdienstleisters unmittelbar gelöscht.

Darüber hinaus scheinen bei den Datenerhebungen nach dem Geldwäschegesetz die Kundinnen und Kunden häufig nicht entsprechend der gesetzlichen Vorgaben informiert zu werden. Für direkte Datenerhebungen bei Betroffenen, wie sie im Rahmen des GwG typischerweise erfolgen, regelt das BDSG ganz allgemein Unterrichtungs- und Hinweispflichten der verantwortlichen Stelle. Der Betroffene ist hiernach über die Identität der verantwortlichen Stelle, über die Zweckbestimmung(en) der Erhebung und Verwendung sowie grundsätzlich über die Kategorien von Empfängern zu unterrichten. Zusätzlich ist der Betroffene auf die Rechtsvorschriften hinzuweisen, die der verantwortlichen Stelle die Erhebungsbefugnis gewähren, hier also die einschlägigen Paragrafen des Geldwäschegesetzes, und er ist über diese Vorschrift(en) sowie die Folgen einer Verweigerung der Angaben aufzuklären.

17. Ordnungswidrigkeiten/Zwangsverfahren

17.1 Ordnungswidrigkeitsverfahren nach dem Bundesdatenschutzgesetz

Vor dem Hintergrund festgestellter gravierender Verstöße gegen das Datenschutzrecht in der jüngeren Vergangenheit und mit der Absicht, die Durchsetzbarkeit datenschutzrechtlicher Anforderungen zu verbessern, wurden bei der Novellierung der Bestimmungen des Bundesdatenschutzgesetzes (BDSG) auch die Bußgeldvorschriften des § 43 neu gefasst. Insbesondere wurden der Umfang der Ordnungswidrigkeitstatbestände erweitert und die Höhe der Bußgelder, die verhängt werden können, erhöht. Zu den Verstößen, die mit einem Bußgeld belegt sind, zählen jetzt unter anderem nach der zum 1. April 2010 in Kraft getretenen Bestimmung des § 43 Absatz 1 Nummer 8 a BDSG auch die Nichterteilung, die nicht richtige, die nicht vollständige oder nicht rechtzeitige Erteilung von Auskünften an den Betroffenen im Hinblick auf die Erfüllung des Auskunftsanspruchs nach § 34 BDSG.

Nachdem wir im Berichtsjahr mehrfach Verstöße gegen die Auskunftspflicht feststellten, leiteten wir aufgrund dieser neuen Ordnungswidrigkeitsvorschrift wiederholt Ordnungswidrigkeitsverfahren ein. In den betreffenden Fällen hatten sich zuvor Bürgerinnen beziehungsweise Bürger bei uns beklagt, dass ihrem jeweiligen Auskunftsverlangen, selbst wenn sie das um Auskunft ersuchte Unternehmen wiederholt hieran erinnerten, nicht entsprochen wurde. Vor der Einleitung eines Ordnungswidrigkeitsverfahrens, das gegen ein Unternehmen beziehungsweise deren Geschäftsführung betrieben wird, welches über das Internet Softwaredienstleistungen (Downloads = Herunterladen von Dateien) anbietet, hatten sich gleich mehrere Bürger bei uns beklagt, dass das Unternehmen nicht bereit sei, ihnen mitzuteilen, welche Daten über sie gespeichert werden, zu welchem Zweck die Speicherung er-

folgt und ob und gegebenenfalls an wen die Daten weitergegeben wurden beziehungsweise werden. Bei einem anderen Ordnungswidrigkeitsverfahren hatte ein Unternehmen, das als Werbeagentur und als Unternehmensberatung fungiert, dem Auskunftsuchenden derartige von ihm erbetene Auskünfte ebenfalls nicht erteilt. Die Erfüllung des Auskunftsanspruchs des Betroffenen nach § 34 BDSG durch die verantwortliche Stelle ist für den Schutz der Persönlichkeitsrechte unabdingbar. Gleichwohl wird dem Recht des Betroffenen auf Auskunft häufig nicht, wie gesetzlich vorgeschrieben, entsprochen. Wegen der Nichteinhaltung der Auskunftspflicht gegenüber den Betroffenen wurden von uns Geldbußen in Höhe von 1 400 Euro bis 1 600 Euro verhängt. Die erlassenen Bußgeldbescheide wurden bislang zum Teil rechtskräftig.

Die wegen der Nichterteilung von Auskünften betriebenen Ordnungswidrigkeitsverfahren waren darüber hinaus verbunden mit der Verhängung von Bußgeldern aufgrund von Verstößen gegen die Pflicht zur Erteilung von Auskünften an die Aufsichtsbehörde. Für die Erfüllung unserer Aufgaben waren uns Auskünfte, zu denen die betreffenden Stellen verpflichtet sind, nicht erteilt worden.

17.2 Zwangsverfahren der Aufsichtsbehörde

Wie die Zahl der Ordnungswidrigkeitsverfahren stieg im Berichtsjahr auch die der von uns nach dem Bremischen Verwaltungsvollstreckungsgesetz betriebenen Zwangsmittelverfahren weiter an. Zur Durchsetzung datenschutzrechtlicher Anordnungen wurden verstärkt Zwangsgelder festgesetzt. Die Zwangsmittelverfahren wurden in der Regel eingeleitet, weil unserer Aufsicht unterstehende Unternehmen nicht bereit waren, uns die für die Erfüllung unserer Aufgaben benötigten Auskünfte zu erteilen, wozu sie nach § 38 Absatz 3 Satz 1 Bundesdatenschutzgesetz verpflichtet sind. Die Höhe der wegen der Nichteinhaltung der Auskunftspflicht verhängten Zwangsgelder betrug im Fall der erstmaligen Festsetzung jeweils circa 600 Euro. In mehreren Fällen reichte die Festsetzung eines Zwangsgeldes nicht aus. Die betreffenden Unternehmen waren trotz des Zwangsgeldes nicht bereit, ihrer Auskunftsverpflichtung nachzukommen, was die Festsetzung weiterer höherer Zwangsgelder erforderlich machte. Die Verfahren gegen diese Unternehmen sind noch nicht abgeschlossen.

18. Datenschutz auf europäischer und internationaler Ebene

18.1 EUROPOL

Seit dem 1. Januar 2010 gilt der europäische Beschluss des Rates zur Errichtung eines Europäischen Polizeiamts (EUROPOL-Beschluss). Das Recht auf Auskunft des Betroffenen über seine Daten soll sich wie bisher nach den jeweiligen mitgliedstaatlichen Rechtsvorschriften richten. Von Bedeutung sind inhaltliche Änderungen wie:

— die neue, erweiterte Zuständigkeit für schwere Kriminalität (Liste von Straftaten) und für Terrorismus. Damit entfällt die bisherige, eingeschränkte Zuständigkeit für Straftaten im Zusammenhang mit organisierter Kriminalität und Geldwäsche,

— die Aufgabe zur Unterstützung eines Mitgliedstaats der Europäischen Union (EU) bei Ermittlungen von Straftaten, die mithilfe des Internet begangen wurden,

— die Möglichkeit der Errichtung und Nutzung anderer Datenverarbeitungssysteme und

— die Bestellung eines Datenschutzbeauftragten bei EUROPOL.

Im August 2010 ist das Abkommen zwischen der EU und den Vereinigten Staaten von Amerika (USA) über die Verarbeitung von Zahlungsdaten und deren Übermittlung aus der EU an die USA in Kraft getreten. Gemäß diesem Abkommen werden EUROPOL eine Reihe von Aufgaben zugewiesen.

18.2 Mitteilungen der Europäischen Kommission

Die Kommission hat für den Bereich Freiheit, Sicherheit und Recht mehrere wichtige Mitteilungen herausgegeben. Eine Mitteilung über die Politik der Europäischen Union (EU) zur Terrorismusbekämpfung vom 20. Juli 2010 (Kommissionsdokument [2010] 386; Bundesratsdrucksache 462/10) präsentiert eine EU-Strategie zur Terrorismusbekämpfung, beruhend auf den vier Säulen Prävention, Schutz, Verfolgung und Reaktion. In einer weiteren Mitteilung wird ein nützlicher Überblick über das

Informationsmanagement im Bereich Freiheit, Sicherheit und Recht (Kommissionsdokument [2010] 385) gewährt. Es werden die EU-Instrumente aufgezählt, mit denen das reibungslose Funktionieren des Schengen-Raums und der Zollunion gefördert werden soll, wie zum Beispiel die Schengener-Informations-Systeme I und II, die europäische Datenbank zur Speicherung von Fingerabdrücken von Asylbewerbern und Drittausländern (EURODAC), das Visainformationssystem, die Übermittlung von „Advanced Passenger Information (Vorab Passagierinformationen)“ und das Zollinformationssystem. Auch wird in der Mitteilung über einen Raum der Freiheit, der Sicherheit und des Rechts für die Bürger Europas (Kommissionsdokument [2010] 171, Bundesratsdrucksache 246/10) ein Aktionsplan zur Umsetzung des Stockholmer Programms (vergleiche 32. Jahresbericht, Ziffer 14.2) vorgestellt, der unter anderem Planungen zu einer europäischen Verordnung für Ermittlungen durch Eurojust und zu Mitteilungen der Kommission über die Einrichtung einer europäischen Staatsanwaltschaft, über die Weitergabe von Fluggastdatensätzen an Drittländer, über die Realisierbarkeit eines europäischen Kriminalaktennachweises und über die Realisierbarkeit eines europäischen Fahndungsprogramms zur Bekämpfung der Terrorismusfinanzierung vorsieht.

18.3 Safe Harbor-Abkommen

Das Abkommen über die Grundsätze des sogenannten sicheren Hafens (Safe Harbor-Abkommen) wurde nach dem Inkrafttreten der europäischen Datenschutzrichtlinie 95/46/Europäische Gemeinschaft (EG) zwischen der Europäischen Union (EU) und den Vereinigte Staaten von Amerika (USA) im Jahr 2000 ausgehandelt. Anlass hierfür war die Regelung des Artikels 25 der EG-Datenschutzrichtlinie, wonach die Übermittlung personenbezogener Daten in einen Drittstaat nur dann zulässig ist, wenn dort ein angemessenes Datenschutzniveau gewährleistet wird. Bei den USA als Drittland ist dieses nicht gegeben. Durch das Safe Harbor-Abkommen soll gleichwohl ein angemessenes Datenschutzniveau bei einem amerikanischen Unternehmen sichergestellt werden können, indem sich das betreffende Unternehmen auf die in der Safe Harbor-Vereinbarung vorgegebenen Grundsätze verpflichtet. Durch die Verpflichtung und eine Meldung an die Federal Trade Commission (Bundeshandelskommission) können sich die Unternehmen selbst zertifizieren.

In der Praxis ist das Abkommen jedoch nicht unkritisch zu betrachten. Es fehlt an einer flächendeckenden Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA. Aus diesem Grund weisen die obersten Datenschutzaufsichtbehörden im Beschluss vom 28. bis 29. April 2010 (vergleiche Ziffer 20.1 dieses Berichts) darauf hin, dass sich Daten exportierende Unternehmen bei Übermittlungen an Stellen in die USA nicht allein auf die Behauptung einer Safe Harbor-Zertifizierung des Datenimporteurs verlassen können. Vielmehr muss sich das Daten exportierende Unternehmen nachweisen lassen, dass die Safe Harbor-Selbstzertifizierungen vorliegen und deren Grundsätze auch eingehalten werden.

Im Rahmen unserer Beratung stellten wir fest, dass sich Daten exportierende Unternehmen schnell mit der Safe Harbor-Zertifizierung zufrieden geben und dies sogar dazu führt, dass eine Prüfung der ersten Stufe für entbehrlich erachtet wird. Daher möchten wir an dieser Stelle noch einmal darauf hinweisen, dass, bevor überhaupt die Frage der Angemessenheit des Datenschutzniveaus gestellt wird, zu allererst geprüft werden muss, ob für die Übermittlung der Daten überhaupt ein Erlaubnistatbestand existiert. Bei konzerninternem Datenverkehr kommen als Erlaubnisnorm vor allem § 28 Absatz 1 und § 32 Bundesdatenschutzgesetz in Betracht.

18.4 SWIFT-Abkommen

Trotz deutlicher Kritik seitens der Datenschutzaufsichtsbehörden ist am 1. August 2010 das SWIFT-Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika (USA) in Kraft getreten. Durch dieses Abkommen haben die amerikanischen Sicherheitsbehörden die Möglichkeit, zum Zwecke der Terrorismusbekämpfung weitreichend auf die Daten des Finanzdienstleisters SWIFT (Society for Worldwide Interbank Financial Telecommunication) zuzugreifen.

Nach den Anschlägen vom 11. September 2001 begannen die amerikanischen Fahndungsbehörden auf Basis des einheimischen Rechts damit, Einsicht in internationale SWIFT-Transaktionsdaten zu nehmen, um auf diese Weise die Finanzströme potenzieller Terrorgruppen aufzudecken. Die Einsichtnahme erfolgte ohne

hinreichende Rechtsgrundlage. Durch das SWIFT-Abkommen haben die USA jetzt eine völkerrechtliche Grundlage für ihren Zugriff auf europäische Bankdaten.

Aus verfassungs- und datenschutzrechtlicher Sicht ist ein solcher Zugriff höchst bedenklich. Denn die USA können auf Finanzdaten zugreifen, ohne dass gegen die Betroffenen ein hinreichend konkreter Tatverdacht besteht und ohne dass sie an Terroraktivitäten oder an deren Unterstützung mitwirkten oder beteiligt waren. Dazu kommt, dass diese Finanzdaten in den USA fünf Jahre gespeichert bleiben und dort keiner unabhängigen Datenschutzkontrolle unterworfen sind. Anders als in Europa gibt es in den USA nur ein sehr eingeschränktes Datenschutzrecht, nahezu keine datenschutzrechtlichen Garantien für die Bürgerinnen und Bürger und auch keine Betroffenenrechte, die es den Einzelnen erlauben, sich angemessen gegen die Datenverarbeitung in den USA zu wehren. Schließlich können die Betroffenen nicht nachvollziehen, was mit ihren Daten in den USA passiert und ob diese nicht gegebenenfalls an Dritte weitergeleitet werden.

19. Die Entschließungen der Datenschutzkonferenzen im Jahr 2010

19.1 Klare gesetzliche Regelungen zur Abrechnung durch private Stellen in der gesetzlichen Krankenversicherung

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. und 18. März 2010)

In seinem Urteil vom 10. Dezember 2008 hatte das Bundessozialgericht nach der damals bestehenden Rechtslage die Einschaltung privater Stellen bei der Abrechnung von ärztlichen Leistungen gegenüber den gesetzlichen Krankenkassen für unzulässig erklärt. Es betonte, dass bei der Einbeziehung von privaten Stellen ebenso detaillierte Regelungen über den Umfang der verarbeiteten Daten und über die erlaubten Datenflüsse vorliegen müssten, wie dies für die klassischen Abrechnungen über die Kassenärztlichen Vereinigungen der Fall ist. Es sei nicht nachvollziehbar, dass gerade bei der Einbeziehung von Privaten an diese geringere Anforderungen gestellt würden als an die öffentlich-rechtlichen Körperschaften. Infolge des Urteils war die Einbeziehung der privaten Stellen nur noch für einen Übergangszeitraum erlaubt.

Um die Abrechnung von Leistungen durch private Rechenzentren nicht einstellen zu müssen, hat der Gesetzgeber hierfür durch das Arzneimittelrechtsänderungsgesetz vom 17. Juli 2009 vorläufige Rechtsgrundlagen in den §§ 120 Absatz 6 und 295 Absatz 1 b Strafgesetzbuch V (StGB) geschaffen, die bis zum 30. Juni 2010 befristet sind. Die Bundesregierung beabsichtigt nunmehr, die Geltung dieser Übergangsregelungen, die den vom Bundessozialgericht formulierten Anforderungen an den Datenschutz nicht entsprechen, um ein weiteres Jahr zu verlängern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für dringend geboten, unverzüglich materielle Vorgaben für die Einbeziehung privater Stellen bei der Abrechnung von ärztlichen Leistungen im Gesetz zu verankern. Dabei müssen präzise Regelungen geschaffen werden, die denselben Schutz der Sozialdaten garantieren, gleich ob die Daten unter Einschaltung privater oder öffentlich-rechtlicher Abrechnungsstellen verarbeitet werden. Die für die Abrechnung zu verwendenden Daten müssen wie bei den herkömmlichen Abrechnungsregelungen für die Patienten transparent verarbeitet und auf das absolut Erforderliche für den konkreten Zweck normativ begrenzt werden. Weiterhin müssen die Datenflüsse in einer Weise definiert werden, dass die Rechte der Versicherten so wenig wie möglich gefährdet werden. Eine Rechtsaufsicht über die Datenverarbeitung ist sicherzustellen. Es ist zu gewährleisten, dass Krankenkassen bei der Beauftragung privater Abrechnungsstellen nicht mehr Sozialdaten erhalten als bei der Abrechnung über die Kassenärztliche Vereinigung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung auf, unverzüglich inhaltliche Vorschläge für eine verfassungskonforme Regelung zu erarbeiten.

19.2 Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. und 18. März 2010)

Die Bundesregierung beabsichtigt, nicht nur die in den vergangenen Jahren durch zahlreiche Gesetze neu geschaffenen Befugnisse und die bestehenden Sicherheits-

dateien, sondern auch die Kooperationszentren, in denen Polizei und Nachrichtendienste zusammenarbeiten, zu evaluieren.

Die Datenschutzbeauftragten des Bundes und der Länder treten dafür ein, die Evaluierung zeitnah und vorbehaltlos nach wissenschaftlichen Kriterien durchzuführen. Kein Vorbild darf die im Mai 2005 vorgenommene „Evaluierung" des Terrorismusbekämpfungsgesetzes 2002 sein. Diese war eine inhaltlich und methodisch defizitäre Selbsteinschätzung. Dagegen enthalten die in verschiedenen Gesetzen aufgenommenen Evaluationsklauseln sinnvolle Ansätze, die es weiter zu entwickeln gilt. Dies betrifft etwa die Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag zu bestellen ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt darauf hingewiesen, dass die Ausweitung der Befugnisse von Polizei und Verfassungsschutz, auch in das Vorfeld der Gefahrenabwehr, zur anlasslosen, oftmals massenhaften Erhebung personenbezogener Daten unbescholtener Bürgerinnen und Bürger führen kann.

Aufgrund der Eingriffsintensität der Regelungen ist eine systematische, ergebnisoffene und wissenschaftlich fundierte Überprüfung auf der Grundlage eines umfassenden Bewertungsansatzes erforderlich. Jede Evaluation, auch die landesrechtlicher Vorschriften, muss auf der Grundlage valider, strukturierter Daten unter Mitwirkung aller relevanten Stellen in einem transparenten Verfahren durch ein unabhängiges Expertengremium erfolgen. Die Nachvollziehbarkeit und Überprüfbarkeit der Evaluierung ist zu gewährleisten. Der Evaluationsbericht muss dem Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen zur Verfügung stellen.

Dazu muss insbesondere Folgendes dargelegt und bewertet werden

— die mit der zu evaluierenden Norm intendierten Ziele,

— die tatsächlich erzielten Wirkungen (beabsichtigte und unbeabsichtigte) sowie die Wirkungszusammenhänge,

— die Auswirkungen auf die Grundrechte von Betroffenen und unbeteiligten Dritten (Eingriffsbreite und -tiefe),

— die Gewährleistung eines effektiven Grundrechtsschutzes, insbesondere im Hinblick auf den absolut geschützten Kernbereich der privaten Lebensgestaltung, sowie die Wahrung des Verhältnismäßigkeitsgebots,

— die Umsetzung von organisations-, verfahrens- und technikorientierten Schutzvorkehrungen (zum Beispiel von Kennzeichnungspflichten, differenzierten Zugriffsberechtigungen, Verwertungsverboten, Prüf- und Löschungspflichten, Richtervorbehalten, Benachrichtigungspflichten),

— die Leistung, Wirkung sowie der Erfolg und die Effizienz,

— die Stellung der zu evaluierenden Norm im Gesamtrechtsgefüge sowie ihre Wechselwirkung mit anderen Normen.

Die Evaluierung ist kein statischer, sondern ein dynamischer, entwicklungsoffener Prozess, der einer ständigen Optimierung bedarf.

19.3 Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. und 18. März 2010)

Um das Grundrecht der Bürgerinnen und Bürger auf Datenschutz zu gewährleisten, bedarf es einer unabhängigen Datenschutzkontrolle. Der Europäische Gerichtshof hat festgestellt, dass die Datenschutzaufsichtsbehörden für den nicht öffentlichen Bereich in Deutschland nicht völlig unabhängig sind und die Bundesrepublik Deutschland damit gegen die Verpflichtung aus Artikel 28 der Datenschutzrichtlinie (Richtlinie 95/46/Europäische Gemeinschaft) verstößt (Urteil vom 9. März 2010, C-518/07). Europarechtswidrig ist nicht nur die organisatorische Einbindung zahlreicher Datenschutzaufsichtsbehörden für den nicht öffentlichen Bereich in die jeweiligen Innenministerien, sondern auch die Aufsicht der Regierungen über die Datenschutzbehörden. Darüber hinaus ist eine grundsätzliche Neuordnung der Datenschutzaufsicht in Deutschland geboten. Die Grundsätze dieser Entscheidung zur Unabhängigkeit sind auf die Datenschutzkontrolle der öffentlichen Stellen anzuwenden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Bund und Ländern auf, die Datenschutzaufsicht schnellstmöglich den Vorgaben der Richtlinie entsprechend umzugestalten.

Die Ausgestaltung der Unabhängigkeit der Datenschutzkontrollinstanzen muss insbesondere folgenden Kriterien entsprechen:

— Die Datenschutzkontrollstellen müssen ihre Aufgaben ohne jegliche unmittelbare und mittelbare Einflussnahme Dritter wahrnehmen können.

— Es darf keine Fach- und Rechtsaufsicht geben.

— Auch eine mögliche Dienstaufsicht darf nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzkontrollstellen führen.

— Eine Einflussnahme seitens der kontrollierten Stellen ist auszuschließen.

— Zu einer unabhängigen Amtsführung gehören ausreichende Eingriffs- und Durchsetzungsbefugnisse.

— Um eine unabhängige Wahrnehmung der Tätigkeit der Datenschutzkontrollstellen zu gewährleisten, muss ihnen die notwendige Entscheidungshoheit bei Personal, Haushalt und Organisation zustehen.

19.4 Keine Vorratsdatenspeicherung!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. und 18. März 2010)

Das Bundesverfassungsgericht bewertet in seinem Urteil zur Vorratsdatenspeicherung vom 2. März 2010 (1 BvR 256/08) die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten als einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt". Weil diese Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch aller Bürgerinnen und Bürger ermöglicht, lehnt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Vorratsdatenspeicherung grundsätzlich ab. Das Verbot der Totalerfassung gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, die auch in europäischen und internationalen Zusammenhängen zu wahren ist. Die Konferenz fordert deshalb die Bundesregierung auf, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/ Europäische Gemeinschaft einzusetzen.

Darüber hinaus betont das Bundesverfassungsgericht, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Daher strahlt die Entscheidung über den eigentlichen Entscheidungsgegenstand hinaus und muss auch in anderen Bereichen, etwa bei der diskutierten Speicherung der Daten von Flugpassagieren oder bei der Konzeption von Mautsystemen beachtet werden. Auch die zentrale Datenbank für das elektronische Entgeldnachweisverfahren (ELENA) muss jetzt auf den Prüfstand. Der Gesetzgeber ist bei der Erwägung neuer Speicherungspflichten oder -berechtigungen im Hinblick auf die Gesamtheit der verschiedenen Datensammlungen zu größerer Zurückhaltung aufgerufen.

19.5 Körperscanner – viele offene Fragen

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. und 18. März 2010)

Der Anschlagsversuch von Detroit am 23. Dezember 2009 hat die Diskussion über den Einsatz von sogenannten Körperscannern bei der Passagierkontrolle am Flughafen neu entfacht. Mit dieser Technik sollen Sicherheitslücken geschlossen werden. Es ist aber noch weitgehend unklar, was diese Geräte technisch leisten können und wie sie sich in ein konsistentes Gesamtsystem zur Flugsicherheit einfügen lassen. Eine Entscheidung über den Einsatz solcher Geräte, die der Gesetzgeber zu treffen hätte, setzt zumindest die Erfüllung folgender Bedingungen voraus:

1. Es muss geklärt werden, ob mit diesen Geräten ein nennenswerter Sicherheitsgewinn erzielbar ist. Derzeit bestehen zumindest ernsthafte Zweifel an der technischen Leistungsfähigkeit und Effizienz dieser Technologie, vor allem im Hin-

blick auf die Detektierbarkeit von Materialien mit geringer Dichte, etwa pulverförmigen Substanzen, wie sie im Fall des Anschlagsversuchs von Detroit verwendet worden sind.

2. Es muss sichergestellt sein, dass die beim Einsatz der Körperscanner erhobenen Daten der Kontrollierten über den Scanvorgang hinaus nicht gespeichert werden. Auch die Anzeige der Körperkonturen gegenüber dem Kontrollpersonal und die Speicherung der erstellten Bilder über den Scanvorgang hinaus sind technisch auszuschließen.

3. Selbst wenn die vorstehenden Bedingungen erfüllt werden, darf der Einsatz von Scannern die Grundrechte der Betroffenen, insbesondere die absolut geschützte Menschenwürde und das Recht auf körperliche Unversehrtheit nicht verletzen. So dürften zum Beispiel Geschlechtsmerkmale oder künstliche Körperteile beziehungsweise medizinische Hilfsmittel (etwa Prothesen und künstliche Darmausgänge) nicht angezeigt werden. Gesundheitsschäden sind auszuschließen.

4. Die Erfüllung dieser Bedingungen ist in praktischen Tests und Erprobungen nachzuweisen.

19.6 Beschäftigtendatenschutz stärken statt abbauen

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22. Juni 2010)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass die Bundesregierung nach nahezu 30-jähriger Diskussion den Bereich Beschäftigtendatenschutz gesetzlich regeln will. Angesichts der Bedeutung des Beschäftigtendatenschutzes für Arbeitgeber und Arbeitnehmer sollte im Gesetzgebungsverfahren der Grundsatz „Qualität vor übereilten Regelungen“ gelten. Im Hinblick darauf wäre es verfehlt, den Gesetzentwurf in einem Schnellverfahren ohne gründliche Diskussion durchzupauken. Ein solches Verfahren würde unweigerlich zu handwerklichen Fehlern und zu einer nicht akzeptablen inhaltlichen Unausgewogenheit der Bestimmungen führen. Beides gilt es zu vermeiden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bedauert daher, dass der vom Bundesminister des Innern vorgelegte Entwurf das angestrebte Ziel eines zeitgemäßen und verbesserten Schutzes der Beschäftigten vor Überwachung und übermäßiger Kontrolle in wesentlichen Punkten und Zusammenhängen verfehlt. Zudem bleibt eine ganze Reihe von Fragen und Problemen ungeklärt. Im Ergebnis würden die vorgesehenen Änderungen in zentralen Bereichen des Arbeitslebens eine Verschlechterung des Datenschutzes für die Beschäftigten zur Folge haben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, den vorliegenden Gesetzentwurf grundlegend zu überarbeiten, jedenfalls aber deutlich zu Gunsten des Persönlichkeitsrechts der Beschäftigten zu ändern. Ein Gesetz zur Regelung des Beschäftigtendatenschutzes sollte einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem verfassungsrechtlich geschützten Persönlichkeitsrecht des Beschäftigten schaffen. An diesem Anspruch muss sich ein Beschäftigtendatenschutzgesetz messen lassen, das diesen Namen verdient.

Substanzielle Verbesserungen an dem Entwurf eines Beschäftigtendatenschutzgesetzes sind insbesondere in den folgenden Punkten geboten:

— Die im Gesetzentwurf vorgesehene Erlaubnis zur Datenverarbeitung bei Verhaltens- und Leistungskontrollen ist zu weit gefasst und lädt zur Ausweitung der Kontrolle und Überwachung der Beschäftigten geradezu ein. Sie muss deshalb präzise gefasst werden und ist an strenge Voraussetzungen zu knüpfen, damit die durch höchstrichterliche Rechtsprechung gefestigte Auslegung des derzeitigen Datenschutzrechts im Sinne des Schutzes der Beschäftigten vor übermäßiger Überwachung bestehen bleibt.

— Auch die im Entwurf vorgesehene allgemeine Erlaubnis zur Verarbeitung und Nutzung von Beschäftigtendaten zur „Verhinderung und Aufdeckung von Vertragsverletzungen zulasten des Arbeitgebers, Ordnungswidrigkeiten und Straftaten“ würde den Arbeitgebern sehr weitgehende zusätzliche Befugnisse zur Auswertung und Verknüpfung unterschiedlichster Datensammlungen in die Hand geben. Der Gesetzgeber muss vielmehr klarstellen, dass Maßnahmen,

die zu einer ständigen Kontrolle der Beschäftigten führen oder den Betroffenen den Eindruck einer umfassenden Überwachung am Arbeitsplatz vermitteln – etwa durch ständige Videoüberwachung oder regelmäßige Aufzeichnung, Mitschnitte oder Mithören von Ferngesprächen –, weiterhin zu unterbleiben haben.

— Die Intention des Gesetzentwurfs, den Umfang der in Bewerbungsverfahren und während des Beschäftigungsverhältnisses verwendeten Daten zu begrenzen, wird auch verfehlt, wenn – wie im Entwurf vorgesehen – Arbeitgeber im Internet verfügbare Informationen generell nutzen dürfen, und zwar sogar dann, wenn diese durch Dritte ohne Kenntnis der Betroffenen und somit häufig rechtswidrig eingestellt wurden. Damit wird vom datenschutzrechtlichen Grundsatz der Direkterhebung beim Betroffenen abgewichen und Arbeitgeber werden geradezu dazu eingeladen, im Internet und in sozialen Netzwerken systematisch nach dort vorhandenen Informationen über Bewerber und Beschäftigte zu recherchieren. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet vom Gesetzgeber, dass er die Nutzung derartiger Daten untersagt oder zumindest wirksam begrenzt und die Arbeitgeber dazu verpflichtet, die Betroffenen aktiv – und nicht erst auf Nachfrage – darüber aufzuklären, woher die verwendeten Daten stammen.

— Der Schutz der Beschäftigten vor unangemessener Kontrolle und Überwachung ist gerade bei der zunehmenden Nutzung elektronischer Medien am Arbeitsplatz von besonderer Bedeutung. Es ist eine normenklare, strikte Begrenzung der Einsichtnahme der Arbeitgeber in die elektronische Kommunikation von Beschäftigten unter Berücksichtigung von deren schützenswerten Belangen erforderlich.

— Die im Gesetzentwurf an mehreren Stellen vorgesehene „Einwilligung" der Beschäftigten führt zu einer erheblichen Erweiterung der (Kontroll-)Befugnisse der Arbeitgeber. Diese wären jedoch rechtlich höchst zweifelhaft, weil Einwilligungen im Arbeitsverhältnis in den meisten Fällen mangels Freiwilligkeit nicht rechtswirksam erteilt werden können. Hinzu kommt, dass im Gesetzentwurf an keiner Stelle definiert ist, welche Anforderungen an die Rechtswirksamkeit von Einwilligungen im Arbeitsverhältnis zu stellen sind.

19.7 Erweiterung der Steuerdatenbank enthält große Risiken

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Juni 2010)

Bundesrat und Bundestag beraten in Kürze über die im Jahressteuergesetz 2010 vorgesehenen ergänzenden Regelungen zur Erweiterung der zentralen Steuerdatenbank. Die Datenbank soll um elektronische Lohnsteuerabzugsmerkmale (ELStAM), wie zum Beispiel sensible Angaben zu Religionszugehörigkeit und Familienangehörigen, ergänzt werden. Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, diese Regelungen kritisch daraufhin zu prüfen, ob sie datenschutzrechtlichen Belangen genügen und die Rechte der betroffenen Arbeitnehmer hinreichend wahren. Folgende Punkte müssen besondere Beachtung finden:

— Vorherige Information der Arbeitnehmer

Mit der Bildung der elektronischen Lohnsteuerabzugsmerkmale ist die Ablösung der Papierlohnsteuerkarte verbunden. Um eine transparente Verfahrensumstellung zu gewährleisten, müssen die betroffenen Arbeitnehmer vor der erstmaligen Anwendung über die sie jeweils konkret betreffenden neuen Merkmale informiert werden. Dies ermöglicht den Arbeitnehmern, etwaige Fehler in der Datenerfassung beim Bundeszentralamt für Steuern vor dem Datenabruf durch den Arbeitgeber zu korrigieren.

— Keine Speicherung auf Vorrat

In der zentralen Datenbank sollen auch Datensätze zu Personen erfasst werden, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Die Speicherung von Datensätzen auf Vorrat ist verfassungsrechtlich höchst fragwürdig. Im Rahmen eines anlassbezogenen Vorgehens sollten Datensätze nur zu solchen Personen gespeichert werden, die tatsächlich lohnsteuerpflichtig sind.

— Verhindern des unzulässigen Datenabrufs

Die gespeicherten Datensätze werden bundesweit circa vier Millionen Arbeitgebern zur Verfügung stehen. Ein Abruf der elektronischen Lohnsteuerabzugsmerkmale soll nur möglich sein, wenn sich der Arbeitgeber oder ein von ihm beauftragter Dritter authentifiziert und seine Steuernummer mitteilt. Das vorgesehene Verfahren muss jedoch gewährleisten, dass nur befugte Arbeitgeber die Datensätze abrufen können. Ob dies tatsächlich erreicht wird, bleibt klärungsbedürftig. Ist ein unzulässiger Datenabruf nicht auszuschließen, sollte der Abruf generell nur unter Mitwirkung des betroffenen Arbeitnehmers möglich sein.

— Kein Start ohne verfahrensspezifisches IT-Sicherheitskonzept

Die erweiterte zentrale Datenbank wird sehr sensible steuerliche Daten von mehr als 40 Millionen Arbeitnehmern enthalten. Ein hoher Standard hinsichtlich der Datensicherheit muss daher spätestens mit Inbetriebnahme gewährleistet sein. Dies setzt voraus, dass ein umfassendes und vollständiges verfahrensspezifisches IT-Sicherheitskonzept vorliegt. Die Erfahrung zeigt, dass die Entwicklung von IT-Sicherheitskonzepten für Datenbanken dieses Umfangs in zeitlicher Hinsicht einen längeren Vorlauf benötigt. Die notwendigen Arbeiten an einem IT-Sicherheitskonzept müssen unbedingt vor dem Aufbau der Datenbank abgeschlossen sein.

19.8 Rundfunkfinanzierung – Systemwechsel nutzen für mehr statt weniger Datenschutz!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2010)

Die Staatskanzleien der Länder bereiten zurzeit den auch von den Datenschutzbeauftragten des Bundes und der Länder seit langem geforderten Systemwechsel bei der Finanzierung des öffentlich-rechtlichen Rundfunks vor. Ab 2013 soll diese nicht mehr durch eine gerätebezogene Abgabe erfolgen, sondern durch einen wohnungsbeziehungsweise betriebsbezogenen Beitrag, der für jede Wohnung nur einmal, unabhängig von der Art und Anzahl der betriebenen Empfangsgeräte, zu entrichten ist und den Betriebe gestaffelt nach ihrer Größe bezahlen sollen. Der Modellwechsel eröffnet die Möglichkeit, sowohl Finanzierungssicherheit für den öffentlich-rechtlichen Rundfunk zu schaffen, als auch endlich die datenschutzrechtlich relevanten Befugnisse beim Gebühreneinzug auf das erforderliche Maß zu begrenzen und den Grundsatz der Datensparsamkeit und -vermeidung bei der Beitragserhebung umzusetzen.

Der Staat ist gehalten, gesetzlich dafür zu sorgen, dass die Datenverarbeitung auf ein Maß beschränkt wird, das für den Zweck der Rundfunkfinanzierung unerlässlich ist. Der zur Anhörung zu dem Modellwechsel vorgelegte Entwurf des 15. Rundfunkänderungsstaatsvertrages (Rundfunkbeitragsstaatsvertrages – RBStV-E) entspricht dem nicht, sondern schafft statt dessen eine Vielzahl von Datenerhebungsbefugnissen für die Beitragserhebungsstelle, die diese nach dem Modellwechsel von der Gebühr zur Wohnungsabgabe nicht mehr benötigt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Staatskanzleien daher auf, den vorgelegten Entwurf noch einmal unter Beachtung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit, Normenklarheit und Datensparsamkeit nachzubessern und dabei insbesondere

— die Datenerhebungsbefugnisse beim Beitragseinzug von Wohnungsinhabern auf das erforderliche Maß zu beschränken, den Direkterhebungsgrundsatz zu beachten und vor allem auf Datenerhebung beim Adresshandel zu verzichten,

— bei Befreiungsanträgen von Wohnungsinhabern aus sozialen Gründen wie Armut oder Behinderung nur die Vorlage einer Bestätigung des Leistungsträgers zuzulassen, auf die Vorlage der vollständigen Leistungsbescheide aber zu verzichten und

— auf die beabsichtigten Übermittlungen der Adressdaten aller gemeldeten Volljährigen durch die Meldestellen als Einstieg in das neue Beitragsmodell über einen Zeitraum von zwei Jahren zu verzichten, stattdessen die Datenübermittlung auf zeitnahe Übermittlungsbefugnisse nach dem Melderecht zu beschränken.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auch auf die Stellungnahme hin, die sie zur Anhörung zum 15. Rundfunkänderungsstaatsvertrag abgegeben hat.

19.9 Förderung des Datenschutzes durch Bundesstiftung

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3. und 4. November 2010)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt zur Kenntnis, dass die Bundesregierung mit Hilfe einer Stiftung den Datenschutz stärken will. Ungeachtet der noch zu klärenden verfassungsrechtlichen Vorfragen wird dieses Ziel von den Datenschutzbeauftragten nachdrücklich unterstützt. Dieses Vorhaben setzt voraus, dass

— die Stiftung ihre Aufgaben unabhängig von den Daten verarbeitenden Stellen und der IT-Wirtschaft wahrnimmt,

— die größtmögliche Transparenz der Tätigkeit garantiert ist und

— die Stiftung eng mit den Datenschutzbehörden des Bundes und der Länder kooperiert.

Die Stiftung kann nur solche Aufgaben übernehmen, die nicht ausschließlich den Datenschutzbehörden zugewiesen sind. Dies gilt insbesondere für die Kontrolle, ob gesetzliche Anforderungen eingehalten werden.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für angezeigt, möglichst frühzeitig in die Überlegungen zur Stellung und zu den Aufgaben der Stiftung einbezogen zu werden. Insoweit bieten sie der Bundesregierung ihre Unterstützung und Mitarbeit an.

19.10 Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3. und 4. November 2010)

Das Energiewirtschaftsgesetz legt fest, dass seit Anfang des Jahres 2010 digitale Zähler in Häuser und Wohnungen eingebaut werden müssen, die den tatsächlichen Energieverbrauch (zum Beispiel Strom und Gas) und die tatsächliche Nutzungszeit messen (Smart Metering). Damit sollen Verbraucher ihren Energieverbrauch künftig besser kontrollieren und steuern können und zur Verbesserung der Energieeffizienz beitragen.

Digitale Zähler ermöglichen die sekundengenaue Erfassung des Verbrauchs. Bei diesen Informationen handelt es sich um personenbezogene Daten, mit denen detaillierte Nutzungsprofile erstellt werden können. Viele Handlungen des täglichen Lebens in der Wohnung führen zumindest mittelbar zum Verbrauch von Energie. In der Nutzung dieser Ressourcen spiegeln sich somit Tagesabläufe wider. Die detaillierte Erfassung des Verbrauchs birgt daher ein hohes Ausforschungspotenzial bezüglich der Lebensgewohnheiten der Betroffenen in sich. Dies gilt in besonderem Maße, wenn neben dem Gesamtverbrauch im häuslichen Bereich auch der Verbrauch einzelner Endgeräte erfasst wird. Zusätzliche Risiken entstehen, wenn die digitalen Zähler zu Steuerungszentralen für im Haushalt betriebene Geräte ausgebaut werden.

Die detaillierte Erfassung des Energieverbrauchs kann zu tiefgreifenden Verletzungen der Persönlichkeitsrechte der Betroffenen führen und sowohl das Recht auf informationelle Selbstbestimmung als auch die verfassungsrechtlich garantierte Unverletzlichkeit der Wohnung beeinträchtigen. Durch die langfristige Aufzeichnung, die Verknüpfungsmöglichkeiten derartiger Verbrauchsprofile mit anderen Daten und ein Auslesen der Daten per Fernzugriff sind weitere Gefährdungen der Privatsphäre der Betroffenen zu befürchten.

Eine effiziente Energiedistribution und -nutzung darf nicht mit datenschutzrechtlichen Beeinträchtigungen einhergehen. Die zur Einführung digitaler Zähler bisher erlassenen Rechtsnormen im Energiewirtschaftsgesetz schützen die Privatsphäre der Betroffenen jedoch nur unzureichend.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine gesetzliche Regelung für die Erhebung, Verarbeitung und Nutzung der durch digitale Zähler erhobenen Verbrauchsinformationen. Eine solche Regelung muss die schutzwürdigen Interessen der Betroffenen berücksichtigen und eine strikte Zweckbindung der erhobenen personenbezogenen Daten vorschreiben. Die Re-

gelung muss zudem sicherstellen, dass die Prinzipien der Transparenz der Datenverarbeitung beachtet und die Betroffenenrechte gewahrt werden.

Die Gewährleistung des Datenschutzes muss dabei bereits bei der Konzeption und Gestaltung der Infrastruktur zur Energiemessung und der technischen Einrichtungen erfolgen. Dies gilt insbesondere für den Grundsatz der Datenvermeidung und für die Datensouveränität der Betroffenen. So ist sicherzustellen, dass detaillierte Verbrauchswerte von Endgeräten unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit direktem oder indirektem Personenbezug an Dritte übermittelt werden. Die Inanspruchnahme von umweltschonenden und kostengünstigen Tarifen darf nicht davon abhängig gemacht werden, dass Betroffene personenbezogene Nutzungsprofile offenbaren.

Für digitale Zähler und intelligente Verteil- beziehungsweise Verarbeitungsnetze (Smart Grids) sind technische und organisatorische Maßnahmen nach dem jeweils aktuellen Stand der Technik zu schaffen, die insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Transparenz bei der Verarbeitung aller Energieverbrauchs-, Steuerungs- und sonstigen Daten sicherstellen. Hierzu gehört auch die Verschlüsselung personenbezogener Verbrauchsdaten. Die Anforderungen an den technischen Datenschutz und die IT-Sicherheit sind durch verbindliche Standards festzuschreiben, die der Sensitivität der Daten und den zu erwartenden Missbrauchsrisiken Rechnung tragen. Für die Datenverarbeitungssysteme ist zudem ein integriertes Datenschutz- und Sicherheitsmanagementsystem aufzubauen.

19.11 Keine Volltextsuche in Dateien der Sicherheitsbehörden

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3. und 4. November 2010)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung und die Landesregierungen auf, volltextbasierte Dateisysteme nur innerhalb der sehr engen verfassungsrechtlichen Grenzen auszugestalten.

Die Sicherheitsbehörden des Bundes und der Länder (Verfassungsschutz, Polizei) bauen zurzeit ihre elektronischen Dateisysteme aus. Dabei beziehen sie auch Daten mit ein, die bisher nur in Akten vorhanden sind, und streben eine umfassende Volltextverarbeitung mit Suchmöglichkeiten an. Nach jedem in einem Dokument vorkommenden Wort oder Datum kann elektronisch gesucht werden, weil das Dokument als Ganzes erfasst wird.

Dies hat gravierende Folgen: In Akten befinden sich auch Daten von Personen, gegen die sich die behördlichen Maßnahmen nicht als Zielperson richten. Auch wer als unbescholtene Bürgerin oder unbescholtener Bürger unwissentlich Kontakt mit einer Zielperson hatte und beiläufig in den Akten genannt wird, wird nun gezielt elektronisch recherchierbar.

Ein solcher Paradigmenwechsel steht im Widerspruch zum geltenden Recht. Danach dürfen die Sicherheitsbehörden nur unter restriktiven Voraussetzungen ausgewählte personenbezogene Daten in automatisierten Dateien speichern und übermitteln. Heute sind die zu speichernden Datenarten und Datenfelder in spezifischen Datei- und Errichtungsanordnungen genau festzulegen. Die Datenschutzbeauftragten müssen zuvor beteiligt werden.

Durch eine Volltextrecherche würden diese datenschutzrechtlichen Sicherungen aufgehoben. Die Zweckbindung der Datenverarbeitung wäre nicht mehr zu gewährleisten. Die gesetzlichen Begrenzungen sind von verfassungsrechtlichem Gewicht. Der Gesetzgeber hat bewusst engere Voraussetzungen vorgegeben, wenn personenbezogene Daten in IT-Systemen gespeichert werden. Denn elektronisch erfasste Daten können, wie das Bundesverfassungsgericht in ständiger Rechtsprechung betont, in Sekundenschnelle umfassend ausgewertet und ohne Rücksicht auf Entfernungen abgerufen werden. Damit würde in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung besonders intensiv eingegriffen, insbesondere wenn die Daten ohne Wissen der Betroffenen erhoben und verarbeitet werden.

Diese verfassungsrechtlich gebotenen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung, insbesondere die informationelle Gewaltenteilung, würden hinfällig, wenn die unbegrenzte elektronische Volltexterfassung sämtlicher Informationen zugelassen würde.

Daran würde sich rechtlich nichts ändern, wenn technische Mechanismen derartige Auswertungen (vorübergehend) erschweren. Denn zum einen sind diese je-

derzeit technisch änderbar. Zum anderen würde eine vorübergehende Erschwerung der Recherchemöglichkeit weder den Eingriff in das Recht auf informationelle Selbstbestimmung noch den Verstoß gegen die vom Bundesverfassungsgericht vorgegebenen Grenzen einer Vorratsdatenverarbeitung beseitigen.

Bestehen diese Datenschutzrisiken schon bei allgemeinen Verwaltungsbehörden, sind sie bei den Sicherheitsbehörden umso gravierender. Dies gilt besonders für den Bereich der Nachrichtendienste, die auch Informationen zu legalem Verhalten und Erkenntnisse mit noch unklarer Relevanz sammeln dürfen. Für die – gegebenenfalls gänzlich unverdächtigen – Betroffenen hätte eine systemweite gezielte Suche möglicherweise gravierende Konsequenzen. Diese Risiken sind bei der Weiterentwicklung der IT-Systeme bereits in der Konzeptplanung zu berücksichtigen und auszuschließen.

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

20.1 Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich vom 28. bis 29. April 2010 in Hannover)

Seit dem 26. Juli 2000 besteht eine Vereinbarung zwischen der Europäischen Union (EU) und dem Handelsministerium (Department of Commerce) der Vereinigten Staaten von Amerika (USA) zu den Grundsätzen des sogenannten sicheren Hafens (Safe Harbor)[1]). Diese Vereinbarung soll ein angemessenes Datenschutzniveau bei US-amerikanischen Unternehmen sicherstellen, indem sich Unternehmen auf die in der Safe Harbor-Vereinbarung vorgegebenen Grundsätze verpflichten. Durch die Verpflichtung und eine Meldung an die Federal Trade Commission (FTC) können sich die Unternehmen selbst zertifizieren. So zertifizierte US-Unternehmen schaffen damit grundsätzlich die Voraussetzungen, dass eine Übermittlung personenbezogener Daten aus Europa an sie unter denselben Bedingungen möglich ist, wie Übermittlungen innerhalb des europäischen Wirtschaftsraumes (EU/EWR). Die FTC veröffentlicht eine Safe Harbor-Liste aller zertifizierten Unternehmen im Internet.

Solange eine flächendeckende Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist, trifft auch die Unternehmen in Deutschland eine Verpflichtung, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe Harbor-Liste geführtes US-Unternehmen übermitteln.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass sich Daten exportierende Unternehmen bei Übermittlungen an Stellen in die USA nicht allein auf die Behauptung einer Safe Harbor-Zertifizierung des Datenimporteurs verlassen können. Vielmehr muss sich das Daten exportierende Unternehmen nachweisen lassen, dass die Safe Harbor-Selbstzertifzierungungen vorliegen und deren Grundsätze auch eingehalten werden. Mindestens muss das exportierende Unternehmen klären, wann die Safe Harbor-Zertifizierung des Importeurs erfolgte. Eine mehr als sieben Jahre zurückliegende Safe Harbor-Zertifizierung ist nicht mehr gültig. Außerdem muss sich das Daten exportierende Unternehmen nachweisen lassen, wie das importierende Unternehmen seinen Informationspflichten nach Safe Harbor[2]) gegenüber den von der Datenverarbeitung Betroffenen nachkommt. Dies ist auch nicht

---

[1]) Entscheidung 2000/520/Europäische Gemeinschaft (EG) der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, Amtsblatt L 215 vom 25. August 2000, Seite 7.

[2]) Informationspflicht: Die Organisation muss Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über sie erhebt und verwendet, wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken. Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig gebeten werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt.

zuletzt deshalb wichtig, damit das importierende Unternehmen diese Information an die von der Übermittlung Betroffenen weitergeben kann.

Diese Mindestprüfung müssen die exportierenden Unternehmen dokumentieren und auf Nachfrage der Aufsichtsbehörden nachweisen können. Sollten nach der Prüfung Zweifel an der Einhaltung der Safe Harbor-Kriterien durch das US-Unternehmen bestehen, empfehlen die Aufsichtsbehörden, der Verwendung von Standard-Vertragsklauseln oder bindenden Unternehmensrichtlinien zur Gewährleistung eines angemessenen Datenschutzniveaus beim Datenimporteur den Vorzug zu geben.

Stellt ein Daten exportierendes Unternehmen bei seiner Prüfung fest, dass eine Zertifizierung des importierenden Unternehmens nicht mehr gültig ist oder die notwendigen Informationen für die Betroffenen nicht gegeben werden, oder treten andere Verstöße gegen die Safe Harbor-Grundsätze zu Tage, sollte außerdem die zuständige Datenschutzaufsichtsbehörde informiert werden.

Eine Schlüsselrolle im Hinblick auf die Verbesserung der Einhaltung der Grundsätze kommt dabei der Zusammenarbeit der FTC mit den europäischen Datenschutzbehörden zu. Hierfür ist es erforderlich, dass die FTC und die europäischen Datenschutzbehörden die Kontrolle der Einhaltung der Safe Harbor-Grundsätze intensivieren. Die mit der Safe Harbor-Vereinbarung beabsichtigte Rechtssicherheit für den transatlantischen Datenverkehr kann nur erreicht werden, wenn die Grundsätze auch in der Praxis effektiv durchgesetzt werden.

20.2 Datenschutz im Verein: Umgang mit Gruppenversicherungsverträgen

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich vom 24. bis 25. November 2010 in Düsseldorf)

Bei sogenannten Gruppenversicherungsverträgen handelt es sich um Rahmenverträge zwischen Vereinen/Verbänden und Versicherungsunternehmen, die den Mitgliedern unter bestimmten Voraussetzungen den Abschluss von Einzelversicherungsverträgen zu günstigeren als den üblichen Konditionen ermöglichen.

Werden für die Werbung zum Abschluss solcher Verträge personenbezogene Daten der Mitglieder an ein Versicherungsunternehmen übermittelt, setzt dies die Einwilligung der Betroffenen voraus.

In Bezug auf Altmitglieder wurde bisher eine Information mittels Avisschreibens mit der Möglichkeit des Widerspruchs für ausreichend gehalten. Die Aufsichtsbehörden stellen fest, dass auch für Altmitglieder die vorherige Einholung einer informierten Einwilligungserklärung erforderlich ist.

20.3 Minderjährige in sozialen Netzwerken wirksamer schützen

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich vom 24. bis 25. November 2010 in Düsseldorf)

Soziale Netzwerke spielen in unserer Lebenswirklichkeit eine zunehmend wichtige Rolle. Minderjährige beteiligen sich in großer Zahl an solchen Netzen. Ihrer besonderen Schutzbedürftigkeit muss über die Anforderungen hinaus Rechnung getragen werden, die grundsätzlich an eine datenschutzgerechte Ausgestaltung solcher Angebote zu stellen sind (vergleiche Beschluss des Düsseldorfer Kreises vom 18. April 2008). Hier besteht ein erheblicher Schutz-, Aufklärungs- und Informationsbedarf:

— Das Schutzniveau sozialer Netzwerke wird wesentlich dadurch bestimmt, dass die Betreiber Standardeinstellungen vorgeben, zum Beispiel für die Verfügbarkeit von Profildaten für Dritte. Minderjährige Nutzer haben häufig weder die Kenntnisse noch das Problembewusstsein, um solche Voreinstellungen zu ändern. Die Aufsichtsbehörden fordern die Anbieter sozialer Netzwerke auf, generell datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch welche die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Portal an Minderjährige richtet oder von ihnen genutzt wird.

— Es muss erreicht werden, dass die gesetzlich beziehungsweise durch die Betreiber vorgegebenen Grenzen für das Mindestalter der Nutzer eingehalten und wirksam überprüft werden. Dies könnte durch die Entwicklung und den Ein-

satz von Altersverifikationssystemen oder Bestätigungslösungen gelingen. Solche Verifikationssysteme lösen zwar ihrerseits Datenverarbeitungsvorgänge aus und müssen berücksichtigen, dass die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym möglich bleiben muss (§ 13 Absatz 6 Telemediengesetz); dies begründet aber kein Hindernis für ihren Einsatz.

— Minderjährigen und ihren Eltern wird die Einschätzung, welche der angebotenen Dienste sozialer Netzwerke altersgerecht sind, wesentlich erleichtert, wenn die Betreiber eine freiwillige Alterskennzeichnung von lnternetinhalten vornehmen. Denkbar ist auch der Einsatz von Jugendschutzprogrammen, die Alterskennzeichnungen automatisch auslesen und für Minderjährige ungeeignete Inhalte sperren. Die Möglichkeiten, die der Entwurf für einen neuen Jugendmedienschutz-Staatsvertrag hierzu anbietet, müssen intensiv genutzt werden.

— Ebenso wichtig ist die Bewusstseinsbildung bei den minderjährigen Nutzern sozialer Netzwerke für die Nutzungsrisiken und für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den respektvollen Umgang mit den Daten anderer. Die Betreiber sozialer Netzwerke, aber auch staatliche Behörden, Schulen und nicht zuletzt die Eltern stehen in der Pflicht, über bestehende datenschutzfreundliche Nutzungsmöglichkeiten aufzuklären.

20.4 Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4 f Absatz 2 und 3 Bundesdatenschutzgesetz

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich vom 24. bis 25. November 2010 in Düsseldorf)

Die obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich haben bei der Kontrolle verantwortlicher Stellen festgestellt, dass Fachkunde und Rahmenbedingungen für die Arbeit der Beauftragten für den Datenschutz (DSB) in den verantwortlichen Stellen angesichts zunehmender Komplexität automatisierter Verfahren zum Umgang mit personenbezogenen Daten nicht durchgängig den Anforderungen des Bundesdatenschutzgesetzes (BDSG) genügen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich weisen darauf hin, dass die Aus- und Belastung der DSB maßgeblich beeinflusst wird durch die Größe der verantwortlichen Stelle, die Anzahl der zu betreuenden verantwortlichen Stellen, Besonderheiten branchenspezifischer Datenverarbeitung und den Grad der Schutzbedürftigkeit der zu verarbeitenden personenbezogenen Daten. Veränderungen bei den vorgenannten Faktoren führen regelmäßig zu einer proportionalen Mehrbelastung der DSB.

Nachfolgende Mindestanforderungen sind zu gewährleisten:

I. Erforderliche Fachkunde gemäß § 4 f Absatz 2 Satz 1 BDSG

§ 4 f Absatz 2 Satz 1 BDSG legt fest, dass zum Beauftragten für den Datenschutz (DSB) nur bestellt werden darf, wer die erforderliche Fachkunde und Zuverlässigkeit besitzt. Weitere Ausführungen dazu enthält das Gesetz nicht. Vor dem Hintergrund der gestiegenen Anforderungen an die Funktion des DSB müssen diese mindestens über folgende datenschutzrechtliche und technisch-organisatorische Kenntnisse verfügen:

1. Datenschutzrecht allgemein – unabhängig von der Branche und der Größe der verantwortlichen Stelle

   — Grundkenntnisse zu verfassungsrechtlich garantierten Persönlichkeitsrechten der Betroffenen und Mitarbeiter der verantwortlichen Stelle und

   — umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung der für die verantwortlichen Stellen einschlägigen Regelungen des BDSG, auch technischer und organisatorischer Art,

   — Kenntnisse des Anwendungsbereiches datenschutzrechtlicher und einschlägiger technischer Vorschriften, der Datenschutzprinzipien und der Datensicherheitsanforderungen insbesondere nach § 9 BDSG.

2. Branchenspezifisch – abhängig von der Branche, Größe oder IT-Infrastruktur der verantwortlichen Stelle und der Sensibilität der zu verarbeitenden Daten

   — Umfassende Kenntnisse der spezialgesetzlichen datenschutzrelevanten Vorschriften, die für das eigene Unternehmen relevant sind,

— Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit (physische Sicherheit, Kryptographie, Netzwerksicherheit, Schadsoftware und Schutzmaßnahmen, et cetera),

— betriebswirtschaftliche Grundkompetenz (Personalwirtschaft, Controlling, Finanzwesen, Vertrieb, Management, Marketing et cetera),

— Kenntnisse der technischen und organisatorischen Struktur sowie deren Wechselwirkung in der zu betreuenden verantwortlichen Stelle (Aufbau- und Ablaufstruktur beziehungsweise Organisation der verantwortlichen Stelle) und

— Kenntnisse im praktischen Datenschutzmanagement einer verantwortlichen Stelle (zum Beispiel Durchführung von Kontrollen, Beratung, Strategieentwicklung, Dokumentation, Verzeichnisse, Logfile-Auswertung, Risikomanagement, Analyse von Sicherheitskonzepten, Betriebsvereinbarungen, Videoüberwachungen, Zusammenarbeit mit dem Betriebsrat et cetera).

Grundsätzlich müssen die erforderlichen rechtlichen, technischen sowie organisatorischen Mindestkenntnisse bereits zum Zeitpunkt der Bestellung zum Datenschutzbeauftragten im ausreichenden Maße vorliegen. Sie können insbesondere auch durch den Besuch geeigneter Aus- und Fortbildungsveranstaltungen und das Ablegen einer Prüfung erlangt sein. Um eventuell zu Beginn der Bestellung noch bestehende Informationsdefizite auszugleichen, empfiehlt sich der Besuch von geeigneten Fortbildungsveranstaltungen. Der Besuch solcher Veranstaltungen ist auch nach der Bestellung angezeigt, um auf dem aktuellen, erforderlichen Informationsstand zu bleiben, und um sich Kenntnisse über die sich ändernden rechtlichen und technischen Entwicklungen anzueignen.

II. Anforderungen an die Unabhängigkeit der/des Beauftragten gemäß § 4 f Absatz 3 BDSG

Gemäß § 4 f Absatz 3 Satz 2 BDSG sind DSB in Ausübung ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Um die Unabhängigkeit der DSB zu gewährleisten, sind eine Reihe betriebsinterner organisatorischer Maßnahmen erforderlich:

1. DSB sind der Leiterin beziehungsweise dem Leiter der verantwortlichen Stelle organisatorisch unmittelbar zu unterstellen (§ 4 f Absatz 3 Satz 1 BDSG). Sie müssen in der Lage sein, ihre Verpflichtungen ohne lnteressenkonflikte erfüllen zu können. Dieses ist durch entsprechende Regelungen innerhalb der verantwortlichen Stelle beziehungsweise vertragliche Regelungen sicher zu stellen und sowohl innerhalb der verantwortlichen Stelle als auch nach außen hin publik zu machen. Den DSB ist ein unmittelbares Vortragsrecht beim Leiter der Stelle einzuräumen.

2. DSB dürfen wegen der Erfüllung ihrer Aufgaben in Hinblick auf ihr sonstiges Beschäftigungsverhältnis, auch für den Fall, dass die Bestellung zum DSB widerrufen wird, nicht benachteiligt werden (vergleiche § 4 f Absatz 3 Satz 3 ff BDSG). Analog muss bei der Bestellung von externen DSB der Dienstvertrag so ausgestaltet sein, dass eine unabhängige Erfüllung der gesetzlichen Aufgaben durch entsprechende Kündigungsfristen, Zahlungsmodalitäten, Haftungsfreistellungen und Dokumentationspflichten gewährleistet wird. § 4 f Absatz 3 BDSG schränkt insoweit die grundsätzliche Vertragsfreiheit ein. Empfohlen wird grundsätzlich eine Mindestvertragslaufzeit von vier Jahren, bei Erstverträgen wird wegen der Notwendigkeit der Überprüfung der Eignung grundsätzlich eine Vertragslaufzeit von ein bis zwei Jahren empfohlen.

3. Datenschutzbeauftragte sind zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit sie nicht davon durch die Betroffenen befreit wurden. Dies gilt auch gegenüber der verantwortlichen Stelle und deren Leiter (§ 4 f Absatz 4 BDSG).

III. Erforderliche Rahmenbedingungen innerhalb der verantwortlichen Stelle zur Fachkunde und Unabhängigkeit des DSB

1. Die Prüfpflichten der DSB (vergleiche § 4 g BDSG) setzen voraus, dass ihnen die zur Aufgabenerfüllung erforderlichen Zutritts- und Einsichtsrechte in alle betrieblichen Bereiche eingeräumt werden.

2. DSB müssen in alle relevanten betrieblichen Planungs- und Entscheidungsabläufe eingebunden werden. Sie führen das Verfahrensverzeichnis (§ 4 g Absatz 2 BSDG) und haben hierfür die erforderlichen Unterlagen zu erhalten.
3. Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde haben die verantwortlichen Stellen den DSB die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen. Bei der Bestellung von externen DSB kann die Fortbildung Bestandteil der vereinbarten Vergütung sein und muss nicht zusätzlich erbracht werden.
4. Internen DSB muss die erforderliche Arbeitszeit zur Erfüllung ihrer Aufgaben und zur Erhaltung ihrer Fachkunde zur Verfügung stehen. Bei Bestellung eines externen DSB muss eine bedarfsgerechte Leistungserbringung gewährleistet sein. Sie muss in angemessenem Umfang auch in der beauftragenden verantwortlichen Stelle selbst erbracht werden. Ein angemessenes Zeitbudget sollte konkret vereinbart und vertraglich festgelegt sein.
5. Die verantwortlichen Stellen haben DSB bei der Erfüllung ihrer Aufgaben insbesondere durch die zur Verfügung Stellung von Personal, Räumen, Einrichtung, Geräten und Mitteln zu unterstützen (§ 4 f Absatz 5 BDSG).

20.5 Umsetzung der Datenschutzrichtlinie für elektronische Kommunikationsdienste

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich vom 24. bis 25. November 2010 in Düsseldorf)

Gegenwärtig wird über die Umsetzung der überarbeiteten Datenschutzrichtlinie für elektronische Kommunikationsdienste („ePrivacy Directive“) in nationales Recht beraten, die bis zum 24. Mai 2011 abgeschlossen sein muss. Die Richtlinie enthält in ihrem Artikel 5 Absatz 3 eine Regelung, die die datenschutzrechtlichen Voraussetzungen auch beim Umgang mit „cookies“ neu festlegt: Die bisherige Opt-Out-Lösung (Widerspruchslösung) wird durch eine Opt-In-Lösung (Einwilligungslösung) mit einer vorherigen umfassenden Information über die Zwecke der Verarbeitung ersetzt. Durch die Änderung der Richtlinie wird nun eine Anpassung des Telemediengesetzes hin zu einer informierten Einwilligung erforderlich, da im geltenden Telemediengesetz eine Widerspruchslösung umgesetzt ist (§ 15 Absatz 3 Telemediengesetz).

Eine solche Änderung stößt auf erhebliche Widerstände auf Seiten des zuständigen Ministeriums, das eine Einwilligungslösung schon durch die in § 12 Absatz 1 und 2 Telemediengesetz (TMG) definierten allgemeinen Grundsätze realisiert sieht. Würde man dieser Auslegung folgen, müsste eine „alte“ Vorschrift zukünftig in „neuer“, zudem auch strengerer Weise ausgelegt und angewendet werden. Dies wäre nur schwer vermittelbar und möglicherweise kaum durchsetzbar.

Die Datenschutz-Aufsichtsbehörden betrachten bei ihrer Kontroll- und Aufsichtstätigkeit im Bereich der Telemedien § 15 Absatz 3 TMG als einschlägig für die Verwendung von „cookies“ in diesem Zusammenhang. Demnach sind Nutzungsprofile nur unter Verwendung eines Pseudonyms und vorbehaltlich eines Widerspruchs des Betroffenen zulässig. Nutzungsprofile werden in der Regel mit Hilfe von „cookies“ erstellt, die im „cookie“ gespeicherte eindeutige Identifikationsnummer (cookie-ID) wird entsprechend als Pseudonym angesehen. Diese Auslegung hat sich in der Praxis bewährt und wird allgemein anerkannt.

Die Umsetzung der „ePrivacy Directive“ erfordert daher eine gesetzliche Anpassung des TMG.

21. Die Europäische und die Internationale Datenschutzkonferenz

Die Entschließungen der Europäischen Datenschutzkonferenz im Jahr 2010 stehen auf der Internetseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter
http://www.bfdi.bund.de/cln_136/DE/Entschliessungen/EuDSK/EUDSK_node.html
zur Verfügung.

Die Entschließungen lauten:

— Geplantes Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Datenschutzstandards im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

— Einsatz von Körperscannern für die Sicherheit an Flughäfen

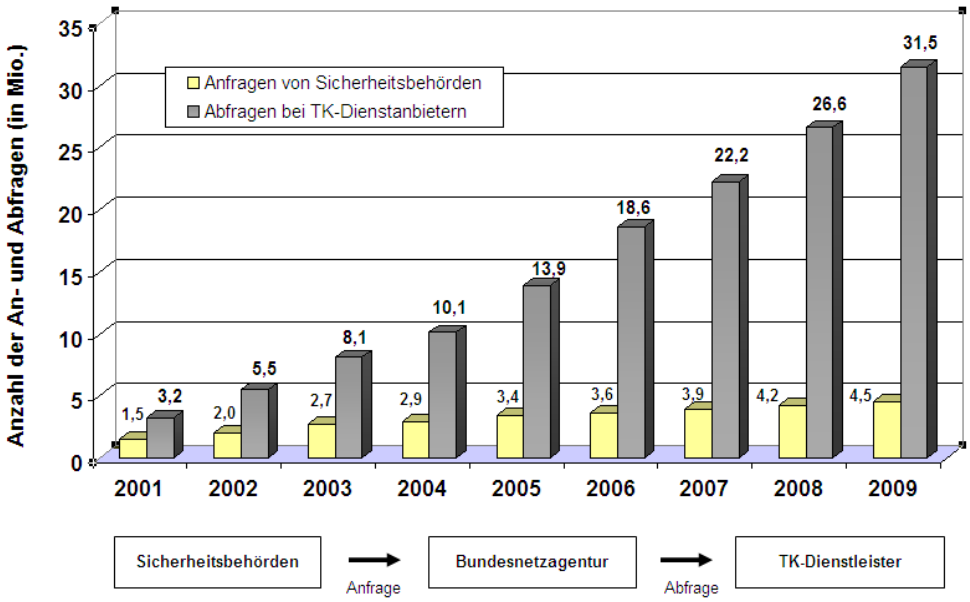
Informationen zur Internationalen Datenschutzkonferenz sind unter http://www.bfdi.bund.de/cln_111/DE/EuropaUndInternationales/GremienOrganisation/Artikel/DieInternationaleDatenschutzkonferenz.html?nn=409534 zu finden.

Die Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation hat im Jahr 2010 eine „Charta zur Regelung der Datennutzung in der digitalen Welt“ verabschiedet. Die Charta befindet sich auf der Internetseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter http://www.bfdi.bund.de/cln_134/SharedDocs/Publikationen/Entschliessungssammlung/WeitereGremien/DieGranadaChartaF%C3%BCrDatenschutzInEinerDigitalenWelt.html?nn=409248

22. Anhang

22.1 Automatisiertes Auskunftsverfahren gemäß § 112 Telekommunikationsgesetz

Sicherheitsbehörden erhalten gemäß § 112 Telekommunikationsgesetz (TKG) über die Bundesnetzagentur von Telekommunikationsdiensteanbietern Auskünfte aus deren Kundendateien (Namen und Anschrift der Inhaber von Rufnummern). Der Kreis der ins automatisierte Verfahren eingebundenen Behörden und verpflichteten Unternehmen wurde im Laufe der Jahre stetig vergrößert. Im abgebildeten Diagramm ist die Entwicklung beim automatisierten Auskunftsverfahren gemäß § 112 TKG im Zeitraum 2001 bis 2009 dargestellt.



Quelle: Tätigkeitsbericht 2009 der Bundesnetzagentur

22.2 Liste des verfügbaren Informationsmaterials

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

22.3 Index

Druck: Anker-Druck Bremen