BREMISCHE BÜRGERSCHAFT **Drucksache 18 / 302**
Landtag 16. 03. 12
18. Wahlperiode

34. Jahresbericht der Landesbeauftragten für Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats über das Ergebnis der Tätigkeit im Jahr 2011 den 34. Jahresbericht zum 31. März 2012 (§ 33 Absatz 1 Bremisches Datenschutzgesetz – BremDSG). Redaktionsschluss für die Beiträge war der 31. Dezember 2011.

Dr. Imke Sommer
Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Inhaltsverzeichnis

1. Gegen die informationelle Fremdbestimmung

Das Grundrecht auf informationelle Selbstbestimmung schützt die Menschen davor, dass nicht sie selbst, sondern andere darüber bestimmen, wer wann was über sie weiß. Wie informationelle Fremdbestimmung aussehen kann, das sollen die folgenden Beispiele aus dem Berichtsjahr 2011 zeigen.

1.1 Romeo und Julia oder: Das „Buch der Gesichter“ (1)

Paris 2011: Romeo und Julia sitzen Arm in Arm auf den Stufen vor Sacre Coeur und genießen den Blick über Paris. Natürlich dürfen ihre Familien nicht wissen, dass sie sich hier getroffen haben. Zu Hause in Genua gibt es trotzdem Ärger: Ihre Familien haben von ihrer heimlichen Zweisamkeit erfahren. Wie 1597 von Shakespeare beschrieben: Großes Drama. Was ist passiert?

Die Familien sind bei einem großen sozialen Netzwerk mit dem Namen „Buch der Gesichter“ angemeldet. Dieses Netzwerk hat im Jahr 2011 seinem Namen alle Ehre gemacht und die Funktion der Gesichtserkennung frei geschaltet. Romeos Familie hat dem Gesichtserkennungsprogramm vielfach bestätigt, dass Fotos von Romeo in Frontalansicht, im Profil, im Halb-, im Viertel-, und im Achtelprofil tatsächlich Romeo zeigen. Dadurch hat sie der Software beigebracht, Romeo auch auf anderen Bildern zu erkennen. Genau das hat Julias Familie mit Fotos von Julia gemacht. Beide Familien haben viel Spaß gehabt, weil das Programm anfangs den bärtigen Kutscher für Julia gehalten hat und Romeo mit der gewichtigen Köchin verwechselt wurde. Durch die ständige Bestätigung von richtigen Zuschreibungen bekam das Programm eine sehr hohe Trefferquote.

Und natürlich hat die Paris-Touristin aus den Vereinigten Staaten von Amerika, die nicht nur Sacre Coeur, sondern auch die Treppe mit den vielen Menschen davor so schön fand, die besten Fotos auf Ihrer Seite im „Buch der Gesichter“ eingestellt. Und während Julia das japanische Paar fotografierte, das so nett mit Händen und Füßen um ein Foto von sich vor Notre Dame gebeten hatte, dokumentierte die Japanerin die Fotoaktion mit dem zweiten Apparat. Natürlich nur, um später erklären zu können, warum sie mit ihrem Liebsten gemeinsam auf dem Foto zu sehen ist. Auch dieses Foto ist ins Internet gelangt. Da war es für die Familien von Romeo und Julia leicht, den Beweis für das unerlaubte Treffen zu führen. Kinkerlitzchen? Die Irrtümer des Gesichtserkennungsprogramms, die im Beispiel von Julia und dem Kutscher witzig waren, verlieren jede Komik, wenn es die mit einem ähnlichen Programm ausgestattete Bomben-Drohne im „Kampf gegen den Terrorismus“ ist, die sich irrt . . .

Besonders erstaunlich ist, dass nach Auffassung des „Buches der Gesichter“, nach Auffassung von facebook, unsere „faces“ (Gesichter) allein dem „book“ (Buch) gehören sollen. Das erfuhr ein Wiener Student, der gegenüber facebook seinen datenschutzrechtlichen Auskunftsanspruch geltend gemacht hatte und eine CD-Rom erhielt, die ausgedruckt 1 200 DIN A4-Seiten umfasste: Chatprotokolle, Browsereinstellungen, Login-Daten, Daten, die er längst gelöscht hatte, und so weiter. Die biometrischen Daten zu seiner Person, die aus seinen Fotos errechnet worden waren, fehlten. In den facebook-Nutzungsbedingungen heißt es zu Fotos: „Du gibst uns eine (. . .) übertragbare, unterlizensierbare, gebührenfreie, weltweite Lizenz für die Nutzung“. Angesichts der europäischen Auffassungen zum Recht am eigenen Bild ist das schon eine erstaunliche Einwilligung, die laut facebook „durch deine Privatsphäreeinstellungen und Anwendungseinstellungen“ abgegeben wird. Ob die Klausel im juristischen Sinn als „überraschend“ anzusehen ist, wird sich zeigen. Im Tatsächlichen überrascht uns in diesem Zusammenhang ja vermutlich nicht mehr so viel.

Mein Hamburger Kollege Prof. Dr. Johannes Caspar hält die gegenwärtige Ausgestaltung der Gesichtserkennungsfunktion bei facebook zu Recht für rechtswidrig. Auf eine rechtfertigende gesetzliche Grundlage kann sich die Nutzung von bei facebook eingestellten Fotos für Gesichtserkennungsprogramme nicht stützen. Eine Rechtfertigung über die Einwilligung derjenigen, deren Gesichter „erkannt“ werden, muss den strengen Anforderungen des Bundesdatenschutzgesetzes genügen. Sie muss bewusst, freiwillig, informiert und schon vor dem Einsatz der Gesichtserkennungssoftware erfolgen. Daten über menschliche Gesichter, die unter Missachtung dieser gesetzlichen Anforderungen entstanden sind, müssen gelöscht werden.

Wir wissen nicht, wie der Konflikt mit facebook über die Gesichtserkennung enden wird. Aber selbst ein Einlenken eines einzelnen Konzerns dürfte nicht das Ende der Diskussion um die Gesichtserkennungsprogramme im Internet bedeuten. Das zeigt die Liste der geförderten Projekte aus dem Themenfeld „Mustererkennung" des Bundesministeriums für Bildung und Forschung. Sie enthält Projekte mit sprechenden Namen wie Automatisierte Detektion interventionsbedürftiger Situationen durch Klassifizierung visueller Muster (ADIS), Analyse von Personenbewegungen an Flughäfen mittels zeitlich rückwärts und vorwärts gerichteter Videodatenströme (APFel) und Mustererkennung und Video Tracking: sozialpsychologische, soziologische, ethische und rechtswissenschaftliche Analysen (MuViT). Die Europäische Union finanziert das Projekt Intelligent information system supporting observation, searching and detection for security of citizens in urban environment (INDECT). Dabei geht es darum, Videoüberwachungssysteme dazu zu befähigen, automatisch strafrechtlich relevante Bedrohungen und Taten zu erkennen. Zu dem vom Bundesministerium für Bildung und Forschung mit 1,2 Millionen Euro geförderten Projekt Parallele Gesichtserkennung in Videoströmen (PaGeVi), einem Verfahren zur Identifizierung gesuchter Personen in Videoströmen, äußert das Bundesministerium in einem Informationsblatt, Gesichtserkennung habe „im Vergleich mit anderen biometrischen Verfahren (. . .) den Vorteil, ohne kooperierende Mitwirkung der zu erkennenden Personen auszukommen". Das scheint eine als „naturalistischer Fehlschluss" beschriebene irrige Ableitung dessen, was sein sollte, aus dem, was ist, zu sein.

Wir müssen uns fragen, ob wir die mit der allgegenwärtigen Beobachtung durch optische Geräte verbundene, vermeintlich ehrlichere Gesellschaft wollen. Wollen wir nicht doch verbergen, dass wir die scheußliche Vase von der Erbtante, die das Gesicht König Ludwigs des Zweiten von Bayern ziert, im Internet versteigert haben? Und dass wir ihr und der Erbaussichten zuliebe mit Bayern-Fanschal beim Spiel, das Werder so schändlich verloren hat, im Bayernfanblock saßen? Ist es uns tatsächlich gleichgültig, dass wir der gesuchten Fahrraddiebin nach Auffassung des Gesichtserkennungsprogramms ähnlich sehen? Wer sagt überhaupt, dass die Menschen, die dem Programm „bestätigen", dass Fotos bestimmte Personen darstellen, dies immer richtig machen (wollen)? Wenn ich nur lange genug Fotos vom Kutscher als Fotos von Julia „bestätige", lernt das Gesichtsprogramm ja auch, aber das Falsche.

Und wir müssen uns fragen, ob es überhaupt darauf ankommen soll, ob jemand etwas zu verbergen hat und ob es in ihrer und seiner Verantwortung bleiben soll, aufwendigste Verbergungsaktionen zu starten. Über die Bewahrung des die menschliche Persönlichkeit mitbestimmenden Rechtes am eigenen Bild müssen wir in Zeiten von immer besser werdenden Gesichtserkennungsprogrammen neu nachdenken. Der Gedanke von den Menschen als „Beiwerk", die nach dem Kunsturheberrechtsgesetz ohne Verletzung ihres Rechts am eigenen Bild einfach zu Gebäuden „dazu fotografiert" werden dürfen, hat sich seit der Verbreitung der pixelscharfen Fototechnik erledigt. Gesichtserkennungsprogramme sind so leistungsfähig, dass sie die Menschen noch im winzigsten Bildausschnitt finden.

Wir brauchen also das Schild auf der Vorderseite des Jahresberichtes. Neben der Durchsetzung der unsere informationelle Selbstbestimmung schützenden Gesetze brauchen wir fotografierfreie und filmfreie Zonen und eine ganz neue Kultur des Fragens, ob die Abgelichteten mit dem Fotografieren und Filmen einverstanden sind. Und diese Kultur muss gleichermaßen im privaten, persönlichen Bereich gelten, wie von staatlichen und privaten Stellen im öffentlichen Bereich gepflegt werden. Gegen die informationelle Fremdbestimmung.

1.2 Die Kommerzialisierung der Privatsphäre oder: Das „Buch der Gesichter" (2)

Constanze Kurz hat gemeinsam mit Frank Rieger das Buch „Die Datenfresser. Wie Internetfirmen und Staat sich unsere Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen" geschrieben. Darin wird anhand des fiktiven Falles der Gründung eines sozialen Netzwerkes für Menschen mit Haustieren beschrieben, worin der Wert der Informationen liegt, die die Mitglieder von sozialen Netzwerken diesen überlassen. Die fiktive, aber vielen tatsächlichen Firmen nachgebildete Firma startet mit 350 000 Euro und ist nach drei Jahren neun Millionen Euro wert. Die Geschäftsidee fußt allein darauf, durch das Setzen von eigenen cookies (Keks heißt auf Englisch cookie) und den Verkauf der Erlaubnis, cookies zu setzen, Infor-

mationen darüber zu erhalten, wann und wie lange die einzelnen Nutzerinnen und Nutzer auf welcher Internetseite verweilen und daraus Verhaltensprofile und Kaufprofile zu erstellen. Die Informationen werden nach allen Seiten hin (auch psychologisch) ausgewertet, für gezielte Werbung selbst genutzt und verkauft. Die im sozialen Netzwerk aktivsten der 500 000 Nutzerinnen und Nutzer werden nach drei Jahren mit je 26 Euro bewertet. Am Ende des dem Schicksal vieler Firmen nachgebildeten Falles werden die zu Nutzerprofilen veredelten Daten des sozialen Netzwerkes an eine andere Firma verkauft. In anderen Fällen landen die unzähligen Daten bei Firmen, die im Rahmen einer Insolvenzversteigerung den Zuschlag erhalten. Die Autorin und der Autor sinnieren am Ende dieser nicht wirklich fiktiven Geschichte darüber, was daraus folgen könnte, dass Produktempfehlungen an die aktiven Nutzerinnen und Nutzer sozialer Netzwerke geradezu aus deren eigenen Gedanken errechnet werden. Sie meinen, auf diese Weise verschwinde die Grenze zwischen Werbung und Manipulation.

In sozialen Netzwerken findet sich also eine unglaubliche Vielzahl im wahrsten Sinne wertvoller Informationen. Das mit gegenwärtig 800 Millionen Mitgliedern größte soziale Netzwerk ist facebook. Der Gründer des sozialen Netzwerkes facebook, Mark Zuckerberg, hat die Auffassung geäußert, die Privatsphäre sei nicht mehr zeitgemäß. Seine ihn selbst betreffenden Datenpreisgaben im „Buch der Gesichter" sind – von den ohne seinen Willen aufgrund von Datenpannen veröffentlichten privaten Angaben einmal abgesehen – also wahrscheinlich Ausdruck seiner eigenen informationellen Selbstbestimmung. Aber das Grundrecht auf informationelle Selbstbestimmung gilt nicht nur für ihn! Jeder Eingriff in das Grundrecht auf informationelle Selbstbestimmung kann nur durch Akte der Selbstbestimmung gerechtfertigt werden. Entweder können dies Gesetze als Ausdruck der kollektiven Selbstbestimmung der Gesellschaft sein, oder es können Einwilligungen sein, die Ausdruck der individuellen Selbstbestimmung jedes Menschen sind. Selbstbestimmt sind aber nach unseren Gesetzen nur diejenigen Einwilligungen, die auf einer vorgängigen bewussten, freiwilligen und informierten Entscheidung beruhen, die jederzeit widerrufen werden kann. Das „Buch der Gesichter" kann sich für seine Datenverarbeitungen für die eben erwähnte Gesichtserkennungssoftware nicht auf rechtfertigende Gesetze berufen. Das gilt auch für andere Funktionen von facebook. Daher muss für jede Erhebung, Speicherung und Übermittlung von Daten und jede sonstige Nutzung jeweils eine rechtswirksame Einwilligung abgegeben worden sein.

Hier hakt es nach der Analyse des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein. In rechtswidriger Weise Fremdbestimmendes wurde bei den „Fanseiten", aber auch beim Hinterherspüren hinter den Internetgewohnheiten der Mitglieder des sozialen Netzwerkes gefunden.

1.2.1 Fanatisches

Nach der facebook-Logik können Personen Mitglieder von facebook werden, also Profilseiten über sich anlegen, wenn sie den Nutzungsbedingungen zustimmen, zu denen es auch gehört, dass sie ihren echten Namen verwenden. Öffentliche und private Stellen können Fanseiten betreiben. Personen untereinander können „Freunde" werden. Personen und Stellen können „Fans" von Fanseitenbetreibern werden. Wenn facebook-Mitglieder Fanseiten besuchen, erhebt facebook die dabei anfallenden Daten. Diese Daten werden aber auch von Nichtmitgliedern erhoben, wenn diese etwa über Suchmaschinen auf die Fanseiten gelangen. Dass im letztgenannten Fall keine rechtswirksamen Einwilligungen vorliegen, liegt daran, dass „Erklärungen" Ahnungsloser schon der Erklärungscharakter abgeht. Wie ist es aber bei den Mitgliedern?

Rechtswirksame Einwilligungen setzen voraus, dass die Betroffenen vor der Datenverarbeitung über die konkrete Erhebung und Verwendung der Daten und über deren Zweck informiert worden sind. Die Einwilligung muss freiwillig und in Kenntnis der Sachlage abgegeben werden und muss jederzeit widerrufen werden können.

Für Mitglieder fingiert facebook die Erteilung der Einwilligung mit der Einrichtung des user account (Nutzerkonto), obwohl während des Anmeldungsprozesses keine klare Information über die Art, den Umfang und den Zweck der Erhebung, Verarbeitung und Nutzung der Daten erfolgt. Die unzähligen Dokumente, auf die facebook verweist, beschreiben die Ziele von Datenerhebungen in vagen Formu-

lierungen und lassen offen, welche Daten zu ihrer Erfüllung erfasst und ausgewertet werden. Informiert ist über die Vielzahl der Datenverarbeitungen bei facebook also niemand und nur informierte Einwilligungen sind rechtswirksam.

Und wie steht es mit der Freiwilligkeit der Einwilligungen? Sie fehlen eindeutig, wenn Studierende gezwungen sind, sich ihre Prüfungsunterlagen bei facebook herunterzuladen, weil sie nur dort erhältlich sind. Hier handelt es sich um von außen kommenden Zwang in einem hierarchischen Verhältnis, der den Betreffenden bewusst ist und dem wegen der drohenden Nachteile nachgegeben wird. Aber wie ist in diesem Zusammenhang sozialer Druck zu bewerten? Wie ist es zu entscheiden, wenn Menschen solchen sozialen Druck (noch) nicht erkennen und sich ihm deshalb nicht entziehen können? Auf diese Fragen danach, wann eine Entscheidung in einem Grad fremdbestimmt ist, dass sie nicht mehr als selbstbestimmt gelten kann und soll, muss unsere Gesellschaft eine Antwort finden.

1.2.2 Das Buch ist uns allen auf der Spur

Das Buch der Gesichter lässt sie kalt? Sie gehören sogar zu denjenigen, die in keinem sozialen Netzwerk angemeldet sind? Sie glauben, dass das der Weg ist, um facebook gegenüber ihre Spur zu verwischen? Wie schon im Zusammenhang mit den Fanseiten erwähnt wurde, geht diese Strategie nicht auf, es sei denn, Sie pflegen eine komplette Internetabstinenz oder löschen ihre cookies regelmäßig. Nach der Untersuchung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein vergibt facebook spezielle cookies. Das passiert nicht nur denjenigen, die ein facebook-Nutzerprofil haben, sondern auch denjenigen, die eine der oben beschriebenen Fanseiten oder eine andere facebook-Seite geöffnet haben. Auf diese Seite können wir alle leicht geraten, weil sie frei über das Netz verfügbar sind und deshalb von Suchmaschinen angezeigt werden. Auf Seiten, die einen „Gefällt-mir"-Button integriert haben, laufen Programme, die uns über den gesetzten cookie identifizieren. Dies geschieht unabhängig davon, ob dieser Knopf angeklickt wird oder nicht. Der cookie hat zwei Jahre Gültigkeit und sammelt in dieser Zeit für facebook Informationen darüber, welche Seiten Sie im Internet ansteuern. Sofern Sie innerhalb der zwei Jahre Mitglied von facebook werden, sind diese Informationen sogar mit ihrem Namen verknüpfbar, weil facebook es ja zur Nutzungsbedingung macht, dass Sie sich mit ihrem echten Namen anmelden. Aber auch ohne ihren Namen sind diese Informationen über Ihr Surfverhalten für viele hochinteressant: Wer hätte gedacht, dass sich in Bremen so viele Menschen gleichzeitig für Pinkelwurst und den Veggi-Day, für Bremen als Hauptstadt des fairen Handels und die Webseite des Billigdiscounters, die ökologische Backkooperative und wegen der besonders wohlschmeckenden Krossen den Discountbäcker, Werder Bremen und Skiurlaub in Bayern interessieren? Die eine Hälfte dieser Informationen wollen wir vielleicht doch lieber für uns behalten und wenden uns deshalb gegen die informationelle Fremdbestimmung.

1.2.3 Keine Alleinverantwortung beim Plattformbetreiber

Wer aber ist rechtlich verantwortlich, wenn facebook durch das Berufen auf unwirksame Einwilligungen beziehungsweise durch Datenerhebungen über Ahnungslose gegen deutsches und europäisches Datenschutzrecht verstößt? Trägt facebook die alleinige Verantwortung dafür, dass durch den Besuch auf einer Seite, die den „Gefällt-mir"-Button verwendet, auch Nichtmitglieder im Internet verfolgt werden? Dürfen sich bremische öffentliche und nicht-öffentliche Stellen darauf berufen, sie würden die facebook-Plattform als „Fanpagebetreiber" lediglich nutzen und könnten nicht steuern, welche Daten facebook erhebe und wie facebook damit weiter verfahre? Die Rechtslage ergibt ein eindeutiges Nein. Die die facebook-Plattform nutzenden Betreiberinnen und Betreiber von „Fanseiten" sind datenschutzrechtlich verantwortlich und im Sinne des Telemediengesetzes verantwortliche Diensteanbieter. Sie können sich dieser rechtlichen Verantwortung nicht unter Hinweis auf die Allmacht facebooks entziehen.

Fanseitenbetreiber können dieser rechtlichen Verantwortung aus rein tatsächlichen Gründen nicht genügen: Nach § 13 Absatz 1 des Telemediengesetzes muss der Diensteanbieter die Nutzerinnen und Nutzer vor der Nutzung in allgemein verständlicher Form über Art, Umfang und Zweck der Erhebung und Verwendung der personenbezogenen Daten und gegebenenfalls darüber informieren, dass Daten außerhalb der Europäischen Union verarbeitet werden. Diesen Pflichten können Fan-

seitenbetreiber gegenwärtig nicht nachkommen, weil facebook sie und uns alle darüber nicht ausreichend informiert. Nach § 13 Absatz 2 des Telemediengesetzes müssen Diensteanbieter sicherstellen, dass die Einwilligung zur Erhebung und Speicherung personenbezogener Daten bewusst und eindeutig erklärt und protokolliert wird und jederzeit abrufbar und widerrufbar ist. Auch diesen Pflichten können Fanpagebetreiber nicht nachkommen, weil facebook – von den rechtlichen Zweifeln an der Wirksamkeit solcher „Einwilligungen" einmal abgesehen – dafür keine ausreichenden Möglichkeiten bereitstellt. Gleiches gilt für die technischen und organisatorischen Vorkehrungen für die Löschung durch den Diensteanbieter, die Diensteanbieter nach dem Telemediengesetz zu treffen haben. Hinzu kommt, dass facebook ohne Zutun und häufig auch ohne Wissen der Fanseitenbetreiber durch den bloßen Aufruf der Fanseite durch Mitglieder oder Nichtmitglieder die beschriebenen Daten erhebt. Zwar erlaubt das Telemediengesetz Diensteanbietern die Datenerhebung für Nutzungsprofile für Zwecke der Werbung, der Marktforschung oder der bedarfsgerechten Gestaltung der Seite. Voraussetzung dafür ist aber, dass Pseudonyme verwendet werden und die Nutzerinnen und Nutzer nicht widersprochen haben. Eine solche Widerspruchsmöglichkeit besteht gegenwärtig nicht, sodass Fanseitenbetreiben auch hier wieder zwangsläufig gegen das Telemediengesetz verstoßen.

Daher hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die öffentlichen Stellen aufgefordert, von der Nutzung von Social Plugins, gemeint sind damit Erweiterungen für externe Seiten, die ein Teilen der Inhalte mit Gruppen in sozialen Netzwerken ermöglichen sollen, abzusehen und auf solchen Plattformen keine Profilseiten oder Fanpages einzurichten. Wir finden, dass es nicht sein kann, dass die Bürgerinnen und Bürger, die sich auf den Seiten öffentlicher Stellen informieren wollen, mit ihren Daten dafür bezahlen. Öffentliche Stellen müssen mit gutem Beispiel vorangehen. Es ist widersprüchlich, sich einerseits für Medienkompetenz einzusetzen und auf der anderen Seite die Nutzerinnen und Nutzer der „Fanseiten" öffentlicher Stellen zu zwingen, ihre Daten aus der Hand zu geben, ohne dass jemand außer den Betreibern selbst weiß, was wann mit ihnen geschieht.

Die bremische Verwaltung hat hierauf reagiert und weist in einem ersten Schritt die Nutzerinnen und Nutzer der Fanseite Bremens auf facebook auf die Datenschutzrisiken und – soweit es ihr möglich ist – die Folgen der Nutzung dieser Seite hin. Übrigens befindet sich diese Seite in Gesellschaft von mindestens zwei Fanseiten, die ebenfalls den Anspruch erheben, DIE Fanseite der Freien Hansestadt Bremen zu sein. Mit Schreiben vom 27. Oktober 2011 hat die Senatorin für Finanzen facebook unter Berufung darauf, dass ein datenschutzkonformer Betrieb von Fanseiten für deren Betreiber gegenwärtig nicht möglich ist, aufgefordert, „ihre Angebote den Anforderungen des deutschen Datenschutzrechts entsprechend umzugestalten, um eine weitere Nutzung insbesondere für die öffentliche Hand zu ermöglichen." Die Senatorin für Finanzen geht in ihrem Schreiben davon aus, „dass es auch im Interesse facebooks ist, eine Datenschutzkonformität seiner Angebote herzustellen, da für die Nutzer, zum Beispiel die Betreiber von Fanseiten, alternativ nur das Abschalten der entsprechenden Funktionen in Betracht käme".

Allen voran öffentliche Stellen, aber auch Unternehmen und wir selbst dürfen uns nicht hinter rechtlich höchst fraglichen Einwilligungen verstecken. Wir alle müssen den Willen derjenigen respektieren, deren Daten wir facebook schenken, indem wir dort Inhalte zur Verfügung stellen. Gegen die informationelle Fremdbestimmung.

1.3 Wie entrinnen wir der informationellen Fremdbestimmung?

Die Beispiele zeigen Fremdbestimmungsbemühungen, die es darauf anlegen, das Grundrecht der Menschen auf Selbstbestimmung darüber, wer wann was von ihnen weiß, zu verletzen. Die Selbstbestimmung im Bereich der Informationen steht aber nicht für sich allein, sondern gehört zur allgemeinen Selbstbestimmung der Menschen. Selbstbestimmung drückt sich darin aus, mutig alles zu hinterfragen, was als vermeintliche Alternativlosigkeit präsentiert wird. Selbstbestimmung setzt voraus, rechtlichen, wirtschaftlichen und sozialen Druck im ersten Schritt zu erkennen und sich ihm dann entgegenzustellen. Selbstbewusst über sich selbst bestimmende Menschen können und wollen im demokratischen Gemeinweisen an der gemeinsamen Selbstbestimmung der Gesellschaft mitwirken. Genau das brauchen wir. Wie in anderen gesellschaftlichen Bereichen sollten wir deshalb auch im Be-

reich der informationellen Selbstbestimmung die Menschen um ihrer selbst Willen wertschätzen. Dafür müssen wir alle auf das Fremdbestimmen verzichten, die Selbstbestimmung der anderen respektieren und Räume schaffen, in denen die Menschen Selbstbestimmungsmut entwickeln und sich von Fremdbestimmung befreien können.

Dr. Imke Sommer

Die Landesbeauftragte für Datenschutz und
Informationsfreiheit der Freien Hansestadt Bremen

2. Bremische Bürgerschaft – Ergebnisse der Beratungen des 33. Jahresberichts

Der Bericht und Antrag des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zum 33. Jahresbericht der Landesbeauftragten für Datenschutz vom 25. März 2011 (Drucksache 17/1708) und zur Stellungnahme des Senats vom 23. August 2011 (Drucksache 18/37) lag zum Redaktionsschluss noch nicht vor.

3. Behördliche und betriebliche Beauftragte für den Datenschutz

3.1 Workshops der behördlichen Datenschutzbeauftragten

Im Berichtsjahr wurde die Reihe der Workshops mit den behördlichen Datenschutzbeauftragten fortgesetzt. Es fanden zwei Workshops, in Bremen mit den Datenschutzbeauftragten der bremischen Verwaltung und in Bremerhaven mit den Datenschutzbeauftragten der dortigen Stadtverwaltung, statt, wobei der Workshop in Bremen wegen des großen Interesses an der Veranstaltung jeweils zweimal mit dem gleichen Schwerpunktthema durchgeführt wurde.

Der erste Workshop befasste sich schwerpunktmäßig mit dem Thema „Datenschutz im Internet – was muss beachtet werden?“. Die Bekanntgabe personenbezogener Daten im Internet ist mit zahlreichen Datenschutzfragen verbunden. In dem Workshop wurden vor allem die rechtlichen und technischen Aspekte des Themas erörtert. Diskutiert wurde insbesondere, unter welchen Voraussetzungen personenbezogene Daten im Internet veröffentlicht werden dürfen, mit welchen Gefahren die Nutzung des Internets verbunden ist und welche Sicherheitsanforderungen eingehalten werden müssen. Erläutert wurden in diesem Zusammenhang die sich aus dem Telemediengesetz und die sich aus den allgemeinen Datenschutzgesetzen ergebenden Vorschriften. In technischer Hinsicht wurde insbesondere die aktuelle Situation der Internetkommunikation im Bremer Verwaltungsnetz näher beleuchtet. Das Thema gab den Teilnehmerinnen und Teilnehmern des Workshops Anlass zu lebhaften Diskussionen. Von der Möglichkeit, Fragen zum Thema zu stellen, wurde rege Gebrauch gemacht.

Der zweite Workshop befasste sich schwerpunktmäßig mit dem Thema „facebook-Kommunikation unter Freunden?“. Mit Hilfe der Plattform facebook können soziale Netzwerke erstellt und betrieben werden, die Menschen mit ihren Freundinnen und Freunden, Arbeitskolleginnen und Arbeitskollegen und anderen Personen verbinden sollen. Auch öffentlichen Stellen bietet facebook die Möglichkeit, „Fanpages“ zu führen und „Social Plugins“ (soziale Erweiterungsmodule) zu nutzen. Gleichzeitig wird über das soziale Netzwerk in erheblichem Maße in das informationelle Selbstbestimmungsrecht der Nutzerinnen und Nutzer eingegriffen. Dabei bleiben wichtige Rechte der Betroffenen unberücksichtigt. Als problematisch erweist sich dabei insbesondere, die sich aus den deutschen Datenschutzgesetzen ergebenden Rechte auf facebook durchzusetzen. Zu kritisieren sind insbesondere die fehlende Transparenz hinsichtlich der personenbezogenen Datenverarbeitung, die mangelnde Umsetzung der Auskunftsrechte der Betroffenen, die Nutzung von Fotos für Zwecke der Gesichtserkennung, die mangelnde Umsetzung der Bestimmungen des Telemediengesetzes sowie das Fehlen erforderlicher technischer und organisatorischer Sicherungsmaßnahmen. Auch dieses Thema stieß bei den behördlichen Datenschutzbeauftragten auf große Resonanz. In den Workshops kam es zu umfangreichen Diskussionen, an denen die Teilnehmerinnen und Teilnehmer mit großem Interesse mitwirkten.

Die Teilnehmenden hatten darüber hinaus in allen Workshops die Möglichkeit, sich über die bei ihrer Tätigkeit gesammelten Erfahrungen auszutauschen. Auch im Jahr 2012 sollen die Workshops mit den behördlichen Datenschutzbeauftragten fortgesetzt werden.

3.2 Die Unverzichtbarkeit der Datenschutzbeauftragten

Den behördlichen und betrieblichen Datenschutzbeauftragten kommt im Hinblick auf die Einhaltung der Vorschriften des Datenschutzes besondere Bedeutung zu. Ihre Aufgabe ist es, auf die Einhaltung des jeweiligen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz hinzuwirken und dabei in erster Linie präventiv tätig zu werden. Hierzu beraten die Datenschutzbeauftragten die Stellen, für die sie in ihrer Funktion tätig sind, in allen datenschutzrechtlichen und daten-

schutztechnischen Fragen, schulen die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen, kontrollieren die Einhaltung der datenschutzrechtlichen Vorschriften und unterstützen die Betroffenen bei der Wahrnehmung ihrer Datenschutzrechte. Die Datenschutzbeauftragten sind für die Organisation des Datenschutzes unverzichtbar und tragen ganz wesentlich zur Umsetzung der gesetzlichen Anforderungen bei.

Im Berichtsjahr waren wir erneut mit mehreren Fällen befasst, in denen die Wiederbesetzung der Funktion der oder des Datenschutzbeauftragten erst nach wiederholtem Drängen durch die Landesbeauftragte für Datenschutz und Informationsfreiheit erfolgte. Uns entgegen gehalten wurde unter anderem von einer öffentlichen Stelle, dass die Funktion der oder des behördlichen Datenschutzbeauftragten aus dem Personalbudget erwirtschaftet werden müsse und bei einer in der Fachabteilung durchgeführten Organisationsuntersuchung die notwendigen zeitlichen Bedarfe für die oder den Datenschutzbeauftragten nicht anerkannt worden seien. Auch von anderen öffentlichen Stellen erhielten wir die Antwort, dass die Mittelknappheit und die geringen personellen Ressourcen die Besetzung des Amtes nicht zuließen.

Die Einhaltung der datenschutzrechtlichen Anforderungen ist für eine ordnungsgemäße Datenverarbeitung unentbehrlich. Personelle oder finanzielle Engpässe dürfen insbesondere nicht dazu führen, dass Grundrechte wie das Recht auf informationelle Selbstbestimmung des Betroffenen eingeschränkt werden.

3.3 Die Aufgaben der Datenschutzbeauftragten

Den behördlichen beziehungsweise den betrieblichen Datenschutzbeauftragten kommt im Hinblick auf die Organisation und die Umsetzung datenschutzrechtlicher Anforderungen in den Behörden, Unternehmen und sonstigen Stellen elementare Bedeutung zu. Nach dem Bremischen Datenschutzgesetz und dem Bundesdatenschutzgesetz ist es ihre Aufgabe, auf die Einhaltung des jeweiligen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz hinzuwirken. Sie haben insbesondere die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck sind sie über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten und haben die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften des Datenschutzgesetzes sowie anderer Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erforderungen des Datenschutzes vertraut zu machen.

Die Datenschutzbeauftragten sind laut Gesetz bei der Erfüllung ihrer Aufgaben weisungsfrei und dürfen deswegen nicht benachteiligt werden. Die Weisungsfreiheit ist das Kernstück der für die gesetzliche Aufgabenwahrnehmung der Datenschutzbeauftragten unerlässlichen Unabhängigkeit. Die Datenschutzbeauftragten können ihrer Verpflichtung, auf die Einhaltung der Datenschutzregelungen hinzuwirken, wie es erforderlich ist, nur nachkommen, so lang sie die verantwortliche Stelle nicht anweisen kann, wie sie sich zu verhalten haben. Die Datenschutzbeauftragten müssen aufgrund ihrer Unabhängigkeit eigenständig bestimmen können, wie sie ihren gesetzlichen Aufgaben nachkommen. Die verantwortlichen Stellen können ihren Datenschutzbeauftragten lediglich Prüfaufträge erteilen, so lang und so weit diese von ihrem Umfang und von ihrer Dauer her nicht die Erfüllung der gesetzlich vorgesehenen Aufgaben gefährden.

Verschiedentlich, sowohl aus dem öffentlichen als auch aus dem nicht-öffentlichen Bereich, erhielten wir Schreiben zur Bestellung von Datenschutzbeauftragten zur Kenntnis, in denen die von den Beauftragten bei ihrer Tätigkeit zu erfüllenden Aufgaben begrenzend festgelegt worden waren. Dies ist mit der Unabhängigkeit der Datenschutzbeauftragten nicht zu vereinbaren. Die verantwortlichen Stellen haben keine Befugnis, den Beauftragten vorzuschreiben, wie sie ihren Aufgaben nachgehen und welche Konsequenzen sie aus ihren Erfahrungen mit der Verarbeitung ziehen müssen. Wir haben die uns zur Kenntnis gegebenen Bestellschreiben zum Anlass genommen, auf eine Änderung der Bestellung zu drängen und die von den Datenschutzbeauftragten wahrzunehmenden Aufgaben den gesetzlichen Vorgaben anzupassen. Die betreffenden Stellen sind unserer Aufforderung nachgekommen.

4. Datenschutz durch Technikgestaltung und Technikbewertung

4.1 Gestaltungsmöglichkeiten datenschutzrechtlicher Verantwortung beim Einsatz technischer Dienstleister

In den letzten beiden Berichtsjahren betrachteten wir die datenschutzrechtliche Verpflichtung zur Übernahme der Verantwortung für Informationstechnologie-Verfahren und die Möglichkeiten ihrer tatsächlichen Wahrnehmung in vernetzten Systemen unter dem Gesichtspunkt des Erfordernisses eines wirksamen Managements (siehe 32. Jahresbericht, Ziffer 4.1) und der tatsächlichen Möglichkeiten der Wahrnehmung dieser Verantwortung im Rahmen der Auftragsdatenverarbeitung durch Definition der sicherheitstechnischen Anforderungen und der Durchführung entsprechender Kontrollen (siehe 33. Jahresbericht, Ziffer 4.4). Die unter Ziffer 4.5 in diesem Jahresbericht skizzierten Probleme im Rahmen des „Cloud Computing“ sind in Bezug auf eine Auflösung der Verantwortlichkeit auch in der Gestaltung des einfachsten Falls, des Outsourcing (Abgabe von Unternehmensaufgaben und Unternehmensstrukturen an Drittunternehmen) von Informationstechnologie-Prozessen auf externe Dienstleister, zu erkennen.

Im Berichtsjahr stellten wir mit der Senatorin für Finanzen erste Überlegungen dazu an, wie die Auftraggeberposition Bremens gegenüber der Anstalt öffentlichen Rechts Dataport als der zentralen Informationstechnologie-Dienstleisterin der Freien Hansestadt Bremen datenschutzrechtlich zu definieren ist. Um die datenschutzrechtliche Verantwortlichkeit für bremische Anforderungen zu bündeln, wurde die Überlegung geprüft, die Befugnisse als Auftraggeber zur Sicherstellung einer datenschutzgerechten Infrastruktur auf die Senatorin für Finanzen zu übertragen. Das Bremische Datenschutzgesetz steht dem allerdings entgegen: Die datenschutzrechtliche Verantwortlichkeit bleibt bei der verantwortlichen Stelle. Eine Aufteilung oder Übertragung der Verantwortlichkeit auf andere Stellen kommt nicht in Betracht. Für die Praxis bedeutet dies, dass jede öffentliche Stelle, die personenbezogene Daten verarbeitet, selbst für die Festlegung der technisch-organisatorischen Maßnahmen und deren Überprüfung vor Ort bei Dataport zuständig ist. Eine „Bündelung“ von Verantwortung kann es so nicht geben. Die Verantwortung bleibt immer bei der Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder diese Datenverarbeitung im Auftrag vornehmen lässt. Wir teilten aber die dem Vorschlag der „Bündelung“ von Verantwortung zugrundeliegende Annahme, dass viele Verfahren gleicher Schutzstufe mit einer für diese Verfahren wirksamen Sicherheitsarchitektur angemessen geschützt werden können. Allerdings ist das Grundproblem, nämlich der Kapazitätsunterschied zwischen Auftraggeberinnen beziehungsweise Auftraggeber und Auftragnehmerinnen beziehungsweise Auftragnehmer hinsichtlich der verfügbaren Ressourcen zur Wahrnehmung der datenschutzrechtlichen Verantwortung in Bezug auf die zentrale Sicherheitsarchitektur, nicht auflösbar.

Deshalb liegt die faktische Verantwortung für die Gewährleistung der Ordnungsmäßigkeit der Datenverarbeitung schon längst beim Dienstleister Dataport. Die Verantwortlichkeit für die der Datenverarbeitung zugrundeliegende Systemarchitektur kann nur eingefordert und ausgestaltet werden, wenn diese Verantwortlichkeit datenschutzrechtlich dort verankert wird, wo sie wahrgenommen werden kann. Eine rechtliche Anpassung an technische Entwicklungen unter größtmöglicher Gewährleistung der Schutzziele und der damit verbundenen Erfordernisse kann zu einer innerhalb der vielschichtigen Arbeitsteilung bei Informationstechnologie-Anwendungen klaren Festlegung der Verantwortung und deren Wahrnehmung führen. Anderenfalls besteht zum Beispiel die Gefahr, dass datenschutzrechtlich erforderliche Sicherheitsanforderungen, die über einen standardisierten Grundschutz hinausgehen, aufgrund der dadurch entstehenden zusätzlichen Kosten nicht zum Bestandteil der Auftragsdatenverarbeitung werden. Dies wurde in unserer Anforderung, ein Security service level agreement (SSLA, Sicherheitsdienstleistungsvereinbarung) abzuschließen, bereits deutlich. Darin wird die Nutzung des Dataport Informationssicherheitsmanagements (ISMS) und des Umsetzungsstandes der Sicherheitsmaßnahmen im Kundenverfahren auf Basis von Informationstechnologie-Grundschutz geregelt. Im Entwurf einer SSLA von Dataport zum Verwaltungs-PC (Version 1.1, Stand 2010) ist beispielsweise vorgesehen, dass eine Überprüfung aktueller Sicherheitsmaßnahmen, die außer der Sicherheitskoordinatorin oder dem Sicherheitskoordinator zusätzliches Personal von Dataport binden, nur durch die Bereitstellung zusätzlicher Mittel möglich sein wird. Eine datenschutzrechtliche

Prüfung beim Auftragnehmer darf nicht von finanziellen Mitteln abhängig gemacht werden.

Wir halten es für dringend erforderlich, den Dienstleister vertraglich eng in die datenschutzrechtliche Verantwortung einzubinden.

4.2 Sichere Betriebsinfrastruktur Basis.Bremen (vorher: Verwaltungs-PC)

Der Senatsbeschluss vom 29. November 2011 zur Standardisierung des Informationstechnologie-Supports in der bremischen Verwaltung zur Verbesserung der Sicherheit und Qualität des Informationstechnologie-Betriebs enthält die Aussage, dass „der Aufbau des zur Gewährleistung der Sicherheit erforderlichen Informationstechnologie-Managements, das vor allem durch einheitliche Prozesse gekennzeichnet ist und das es ermöglicht, qualitativ und quantitativ messbare Aussagen zur Sicherheit des Bremer Verwaltungsnetzes und der darin betriebenen Dienste zu erhalten, (. . .) mit vertretbarem Aufwand nur in einer zentralisierten und standardisierten Betriebsorganisation für die Verwaltungsarbeitsplätze und die sie verbindenden Netze möglich (ist)“.

Die Standardisierung des Informationstechnologie-Supports birgt Risiken, die insbesondere aus grundsätzlichen Möglichkeiten weitreichender zentraler Zugriffe entstehen. Gleichzeitig bietet sie eine Chance zur Erstellung erforderlicher Sicherheitskonzeptionen, um wirkungsvolle Konfigurationen und deren Zusammenwirken zu beschreiben und darüber hinaus die dazugehörigen Prozesse zu definieren, mit denen diese praxisnah in enger Verzahnung mit neuen technischen Entwicklungen umgesetzt werden können.

Durch den Senatsbeschluss wurde auch die Grundlage für die Umsetzung unserer Sicherheitsanforderungen zum Verwaltungs-PC (siehe 33. Jahresbericht, Ziffer 4.4.1) in Verbindung mit der Einführung eines Informationstechnologie-Sicherheitsmanagements (siehe 32. Jahresbericht, Ziffer 4.1) geschaffen.

Das uns vorgelegte Betriebskonzept vom Dezember 2011 zur Betriebsinfrastruktur für die Startmigration zum Projekt Basis.Bremen hat von uns immer wieder eingeforderte grundlegende Voraussetzungen für die Standardisierung des Informationstechnologie-Supports für die bremische Verwaltung anerkannt, enthält aber noch keine Lösungen.

So wurden beispielsweise unsere Anforderungen hinsichtlich Funktionalität und Kontrolle der Administrationsumgebung aufgenommen (siehe 31. Jahresbericht, Ziffer 6.4, 32. Jahresbericht, Ziffer 4.2 und 33. Jahresbericht Ziffer 4.3). Darüber hinaus wird die Notwendigkeit der Erstellung von Risikoanalysen insbesondere für eventuelle administratorische Zwischenlösungen und für den in der Migrationsphase entstehenden Parallelbetrieb von neuer und alter systemtechnischer Umgebung festgelegt.

Für die ausstehende Sicherheitskonzeption zum Verzeichnisdienst Active directory, als Grundlage für den Echtbetrieb des Verwaltungs-PC, und für die zu einem sicheren Computerbetrieb an den Arbeitsplätzen erforderlichen Konfigurationen von Gruppenrichtlinien wird eine Prüfung der aus Schleswig-Holstein und Hamburg vorliegenden Konzepte festgelegt. Wir gehen davon aus, dass die Prüfung hinsichtlich der Eignung zur Umsetzung Bremer Sicherheitsziele und direkt bezogen auf die Bremer Infrastruktur detailliert vorgenommen wird.

Unsere Forderung nach dem Abschluss eines Security service level agreement (SSLA, Sicherheitsdienstleistungsvereinbarung), durch das eine Schaffung und Aufrechterhaltung des Sicherheitsniveaus bei Dataport vertraglich sichergestellt werden soll, wird von der Senatorin für Finanzen hinsichtlich ihrer Wirksamkeit, die Sicherheitsziele der Freien Hansestadt Bremen umzusetzen, geprüft.

Darüber hinaus ist das Bremer PKI-Konzept (public-key-Infrastruktur, ein Verzeichnisdienst zur Verteilung und Vorhaltung von elektronischen Schlüsseln zum sicheren Datenaustausch) anzupassen. Es muss im Rahmen des Standardisierungsprozesses hinsichtlich der Erforderlichkeit, Maschinenzertifikate zu verwenden, ergänzt werden.

Die Senatorin für Finanzen sagte zu, die noch offenen Sicherheitsfragen im Migrationsprojekt zu bearbeiten und hat dafür im Rahmen der Projektorganisation ein zentrales und dezentrales Arbeitspaket zur Datensicherheit und zum Datenschutz vorgesehen. Wir werden diesen Prozess intensiv begleiten.

4.3 Anforderungen an den sicheren Betrieb von SAP

Der sichere Betrieb des Systems SAP, in dem derzeit circa 1 700 Benutzerinnen und Benutzer berechtigt sind, war bereits in den vergangenen zwei Berichtsjahren (vergleiche 32. Jahresbericht, Ziffer 10.3 und 33. Jahresbericht, Ziffer 4.1) ein Thema, bei dem wir ein starkes Interesse an der Umsetzung datenschutzrechtlicher und datenschutztechnischer Maßnahmen hatten. Auch in diesem Jahr hat uns dieses Thema begleitet.

Zwar bestand am Anfang des Berichtsjahres noch nicht zu allen datenschutzrechtlichen und datenschutztechnischen Problemen eine Einigung, da wir aber die Erstellung des Berechtigungskonzeptes im Jahr zuvor beratend begleiteten und zahlreiche Vorschläge zur Verbesserung des Datenschutzes Eingang in das Berechtigungskonzept fanden, erwarteten wir von der Umsetzung des Berechtigungskonzeptes eine grundsätzliche Verbesserung des Datenschutzes und befürworteten diese unter der Voraussetzung, dass die aus unserer Sicht noch offenen Fragestellungen zeitnah bearbeitet werden würden.

Leider müssen wir nun berichten, dass das Berechtigungskonzept im laufenden Berichtsjahr nicht umgesetzt worden ist. Lediglich in einigen Detailfragen konnte eine Klärung erfolgen.

Die Senatorin für Finanzen sagte zu, die Berechtigungspflege zukünftig ausschließlich im Entwicklungssystem durchzuführen und dann in die nachfolgenden Qualitätssicherungssysteme und Produktivsysteme zu transportieren. In diesem Zuge sollen auch die bestehenden Berechtigungen des Qualitätssicherungssystems an das Produktivsystem angepasst werden, da es sich bei dem Qualitätssicherungssystem um eine Kopie des Produktivsystems handelt und mit dieser Maßnahme das Schutzniveau des Qualitätssicherungssystems dem des Produktivsystems angepasst wird.

Einigkeit gibt es nun auch bezüglich der Löschfrist der Benutzerstammsätze, die nun auf zehn Jahre, statt bisher 30 Jahre, festgelegt worden ist.

Ungeklärt ist allerdings immer noch die Problematik der Sammelbenutzer, die nicht der üblichen Namenskonvention unterliegen und deren Passwörter mehreren Anwenderinnen und Anwendern gleichzeitig zur Nutzung bekannt sind. Darüber hinaus besteht weiterhin dringender Handlungsbedarf bei den technischen Berechtigungen sowie in den Arbeitsfeldern Support, Basis-Administratoren, Entwickler und Berater. Gerade in diesen Tätigkeitsbereichen sind besonders umfassende Berechtigungen vergeben worden, die geprüft und reorganisiert werden müssen.

Es ist bedauerlich, dass das eigentliche Berechtigungskonzept nicht umgesetzt werden konnte. Dies gilt umso mehr, als dieses Konzept nur einer von mehreren Bausteinen zur Gewährleistung der Gesamtsicherheit der SAP-Systeme ist. Denn nach dem Umzug der SAP-Systeme zu der Anstalt öffentlichen Rechts Dataport nach Hamburg steht auch noch die grundlegende Überarbeitung weiterer Konzepte aus. Dazu gehören das Informationstechnologie-Rahmenkonzept, das Datenschutzkonzept und das Informationstechnologie-Betriebskonzept sowie das in die Zukunft gerichtete Archivierungskonzept.

Zur Umsetzung der genannten erforderlichen Maßnahmen sowie zur anschließenden dauerhaften Aufrechterhaltung des Datenschutzniveaus sind ausreichende personelle Ressourcen erforderlich. Auch aufgrund der bereits eingetretenen starken Verzögerungen erwarten wir nun, dass diesbezüglich zeitnah Folgeprojekte aufgesetzt werden.

4.4 VISkompakt – Zentrales System zur elektronischen Aktenführung

Noch immer stehen wir in Abstimmung mit der Senatorin für Finanzen zum Einsatz der zentralen Dokumentenverwaltung unter VISkompakt. Unsere datenschutzrechtlichen Anforderungen hatten wir bereits in unseren vergangenen Jahresberichten (vergleiche 32. Jahresbericht, Ziffer 4.3 und 33. Jahresbericht, Ziffer 4.2) dargestellt. Insbesondere geht es uns hier um geeignete Konzepte zur Verschlüsselung von sensiblen personenbezogenen Daten, die Erstellung eines Administrationskonzeptes, die Gewährleistung einer revisionssicheren Protokollierung, die Erstellung von Berechtigungskonzepten sowie die Gewährleistung des Trennungsgebots.

In diesem Jahr erhielten wir weitere Unterlagen. Es handelte sich hier um ein Sicherheitskonzept auf Basis des Schutzbedarfs „normal“, ein Rechtekonzept und Rollenkonzept sowie um einen Auszug aus einem Organisationskonzept. Es fanden erste Gespräche und Präsentationen im Zusammenhang mit dieser Dokumentation statt. Wir erwarten derzeit unter anderem Anpassungen am Organisationskonzept sowie die Vorlage des Einsatzkonzeptes. Problematisch ist weiterhin der Verweis auf übergeordnete Basis-Systemkonzepte. Ausstehend sind hier die Ergebnisse der Prüfung dieser Unterlagen durch die Senatorin für Finanzen sowie die Darlegung der datenschutzrechtlich und datenschutztechnisch relevanten Aspekte. Unklarheiten bestehen außerdem bezüglich des Rechtekonzeptes und Rollenkonzeptes sowie der damit verbundenen Gewährleistung des Trennungsgebots und der Einrichtung einer revisionssicheren Protokollierung, die ebenfalls dem Trennungsgebot unterliegen muss.

Besonders eingehen möchten wir auf die Verarbeitung sensibler personenbezogener Daten. Bei VISkompakt handelt es sich um eine Basisinfrastruktur für die bremische Verwaltung. Es ist bei den Überlegungen zur Schutzbedarfsfeststellung dieser Basisinfrastruktur von zentraler Bedeutung, zu betrachten, welche Daten in Zukunft innerhalb von VISkompakt gespeichert und verarbeitet werden könnten. Die untere Grenze an Schutzbedarf zur Erreichung der Schutzziele „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ bei der Verarbeitung personenbezogener Daten stellt selbstverständlich die Schutzbedarfskategorie „normal“ dar. Derzeit ist aber überhaupt nicht abzusehen, welche Arten personenbezogener Daten zukünftig insgesamt durch die Ressorts und Dienststellen innerhalb von VISkompakt gespeichert und verarbeitet werden sollen. Somit ist abzuwägen, ob die vorgesehene Schutzbedarfskategorie „normal“ für die Basis-Infrastruktur VISkompakt ausreichend ist.

Insbesondere kann bei den personenbezogenen Daten, die innerhalb einer Verwaltung verarbeitet werden, davon ausgegangen werden, dass auch besondere Arten personenbezogener Daten betroffen sind. Nach dem Gesetz sind dies Angaben über die rassische und ethnische Herkunft, die politische Meinung, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Je nachdem, von welchem Ressort oder welcher Dienststelle diese und auch andere personenbezogene Daten gespeichert und verarbeitet werden, kann insbesondere bei dem Schutzziel „Vertraulichkeit“ von einer erforderlichen Schutzbedarfskategorie „hoch“ ausgegangen werden. Insbesondere muss in diesem Fall wegen erheblicher Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse der Betroffenen von erheblicher Beeinträchtigung des informationellen Selbstbestimmungsrechts und einer negativen Innenwirkung oder Außenwirkung bei einer Verfehlung des Schutzziels „Vertraulichkeit“ ausgegangen werden.

Es erscheint unrealistisch, dass im Tagesgeschäft eine manuelle „Trennung“ der Daten in die Schutzbedarfskategorien „normal“ und „hoch“ vor Speicherung in VISkompakt durchgeführt wird beziehungsweise überhaupt durchgeführt werden kann. Es kann daher nicht davon ausgegangen werden, dass lediglich Daten mit dem Schutzbedarf „normal“ Eingang in das System VISkompakt finden. Damit VISkompakt also überhaupt für eine breite Zahl von Anwendungen in der bremischen Verwaltung genutzt werden kann, muss auf Basis dieser Überlegungen allgemein die Schutzbedarfskategorie „hoch“ für das Dokumentenmanagementsystem VISkompakt gelten.

Solange der Schutzbedarf „hoch“ für das Dokumentenmanagementsystem VISkompakt nicht umgesetzt ist, halten wir die Verarbeitung sensibler personenbezogener Daten für nicht zulässig. Im Rahmen der Prüfung von Anschlussbedingungen einzelner Dienststellen an VISkompakt sollte die Senatorin für Finanzen dies ablehnen.

4.5 Orientierungshilfe Cloud Computing des Arbeitskreises Technik

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschäftigte sich über ihre Arbeitskreise Medien und Technik mit dem Thema Cloud Computing und veröffentlichte eine Orientierungshilfe hierzu. Die Orientierungshilfe soll den datenschutzgerechten Einsatz dieser Technologie fördern. An der Orientierungshilfe arbeiteten wir mit.

Cloud Computing, ein englischer Begriff der mit „Datenverarbeitung in der Wolke“ übersetzt werden kann, bezeichnet einen aktuellen Trend in der elektronischen

Datenverarbeitung. Dabei wird ein Teil oder auch die gesamte Datenverarbeitung zu externen Dienstleistern ausgelagert. Aber nicht in ein bestimmtes Rechenzentrum, sondern zu einem Dienstleister. Der Dienstleister kann wieder entsprechende Dienstleistungen und Rechenzentrumskapazität bei weiteren Anbietern einkaufen. Die dafür notwendige Basis ist das Internet, das es erlaubt, diese Infrastrukturen so zu nutzen, als wenn die Datenverarbeitung hausintern durchgeführt würde. Auch wenn sie real zeitgleich in international verteilten Standorten geschieht. Dabei ist das alles flexibel: Wird in Spitzenzeiten oder Projekten mehr Rechenleistung benötigt, mieten die Nutzerinnen und Nutzer sie hinzu. Wird die Rechenleistung nicht mehr benötigt, wird sie nicht weiter gemietet. So wird maximale Flexibilität erreicht und nur das abgerechnet, was auch genutzt wurde.

Für den Datenschutz birgt das viele Gefahren. So ist nicht zwingend gewährleistet, dass die Daten innerhalb der Grenzen Deutschlands oder der Europäischen Union (EU) gespeichert oder verarbeitet werden. Für personenbezogene Daten ist das problematisch, teilweise sogar unzulässig. Nur bei der Datenverarbeitung innerhalb der EU kann von einen einheitlichen Datenschutzniveau ausgegangen werden. In Drittstaaten hingegen kann es beispielsweise staatliche Zugriffsrechte auf Datenverarbeitung innerhalb der jeweiligen Staatsgrenzen geben. Die Anforderungen hinsichtlich der Vertraulichkeit, der Integrität und der Verfügbarkeit der personenbezogenen Daten sind in diesen Fällen in der Regel gar nicht oder nur unter äußerst schwierigen Umständen überhaupt zu erfüllen: Vollständige Kontrollierbarkeit, Transparenz und Beeinflussbarkeit der Datenverarbeitung sind nicht gegeben.

Cloud-Services dürfen nur dann in Anspruch genommen werden, wenn die Auftraggeberinnen und Auftraggeber in der Lage sind, ihre Pflichten als verantwortliche Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutzanforderungen und Informationssicherheitsanforderungen geprüft haben. Cloud Computing darf nicht dazu führen, dass Daten verarbeitende Stellen nicht mehr in der Lage sind, die Verantwortung für die eigene Datenverarbeitung zu tragen. Cloud-Anbieter müssen ihr Angebot datenschutzkonform gestalten.

Die Orientierungshilfe ist unter dem folgenden Link auf unserer Homepage zu finden: http://www.datenschutz-bremen.de/pdf/oh_cloud.pdf

4.6 E-Mail-Migration in der bremischen Verwaltung

Im Berichtsjahr wurde die lange und ausführlich vorbereitete Modernisierung des E-Mail-Systems der bremischen Verwaltung (siehe 31. Jahresbericht, Ziffer 6.5) durchgeführt. Innerhalb der bremischen Verwaltung wurde das Projekt als Exchange Migration bezeichnet.

Bei einigen Projekten innerhalb der bremischen Verwaltung, etwa dem Bürgertelefon-Bremen-Projekt, fiel in diesem Zusammenhang auf, dass allgemein anscheinend vermehrt davon ausgegangen wurde, dass E-Mails nach der abgeschlossenen Exchange Migration verschlüsselt innerhalb des Bremer Verwaltungsnetzes (BVN) übertragen werden. Ebenso haben wir Kenntnis davon erlangt, dass im Bereich der Finanzämter ebenfalls davon ausgegangen wurde, dass E-Mails innerhalb des Bremer Verwaltungsnetzes grundsätzlich sicher übermittelt werden können und daher unbedenklich Daten per E-Mail zwischen den Finanzämtern ausgetauscht werden können.

Wir machten in einem Schreiben an die Senatorin für Finanzen deutlich, dass auch nach der abgeschlossenen Exchange-Migration keinesfalls davon auszugehen ist, dass E-Mails innerhalb der bremischen Verwaltung durchgängig verschlüsselt transportiert werden.

Im Rahmen der Exchange-Migration wurde durch die Brekom ein Computerprogramm verteilt, das die entsprechenden Einstellungen an der E-Mail-Software Outlook auf den von der Umstellung betroffenen Arbeitsplatzcomputern vornimmt. Insbesondere hat die Software auch die Einstellung vorgenommen, dass der Datenaustausch zwischen Outlook und dem E-Mail-Server nur verschlüsselt erfolgt. Leider lief das Programm nicht auf allen Arbeitsplatzcomputern ordnungsgemäß durch. In diesen Fällen mussten die entsprechenden Konfigurationen zur E-Mail-Umstellung manuell durchgeführt werden. Dabei war allerdings nicht gewährleistet, dass in allen Fällen die für den beschriebenen verschlüsselten Datenaustausch notwendige Option „Daten zwischen Microsoft Office Outlook und Microsoft Ex-

change Server verschlüsseln“ in allen Fällen aktiviert worden ist. Und auch wenn die Option im Rahmen der Umstellung aktiviert worden ist, kann sie durch die Benutzerinnen und Benutzer von Outlook jederzeit wieder deaktiviert werden. Es kann also nicht davon ausgegangen werden, dass E-Mails innerhalb des BVN immer verschlüsselt transportiert werden. Insbesondere sind dadurch die Anforderungen aus Ziffer 4, Nummer 3 der aktuell gültigen Richtlinie für die Nutzung der Elektronischen Post nicht erfüllt. Dort ist geregelt, dass die Übermittlung sensibler Daten mittels E-Mail nur unter Einsatz geeigneter Verschlüsselungsverfahren zulässig ist. Das beschriebene Verfahren ist aus den genannten Gründen nicht geeignet. Eine Stellungnahme der Senatorin für Finanzen steht noch aus.

4.7 Bericht aus dem Arbeitskreis Technik

Zentrale Themen des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder waren in diesem Jahr beispielweise die Erstellung einer Orientierungshilfe Cloud Computing (vergleiche Ziffer 4.5 dieses Berichts) und das „Löschen im Internet“.

Aus dem Bereich der Forschung wurden bezüglich des „Löschens im Internet“ verschiedene Szenarien und Lösungsansätze für zeitlich begrenzte Veröffentlichungen im Internet vorgestellt. Die Daten werden dabei über kryptografische Verfahren mit einem Verfallsdatum ausgestattet, nach dessen Ablauf sie nicht mehr zu lesen sind. Da bis dahin die Daten aber immer im Klartext zur Verfügung stehen, ist es in der Zeit bis zum Erreichen des Verfallsdatums möglich, die Daten ohne das Verfallsdatum zu kopieren. Das kann nicht verhindert werden. Somit werden dann die Originaldaten mit Erreichen des Verfallsdatums gelöscht, etwaige vorhandene Kopien werden von den Verfahren aber nicht erfasst. „Echte“ Löschfunktionen, die Daten vollständig und unwiederbringlich aus dem Internet entfernen, existieren nicht.

Ein weiteres wichtiges Thema im Arbeitskreis Technik war das neue Internetprotokoll Version 6 (IPv6). Hierbei steigt die Länge der Adressen von ehemals 32 Bit auf 128 Bit. Somit stünden genügend Internetprotokoll-Adressen zur Verfügung, um jedes noch so kleine elektronische Gerät mit mindestens einer weltweit eindeutigen Adresse auszustatten. Dadurch erhöht sich das Risiko, dass Internetnutzerinnen und Internetnutzer identifiziert und ihre Aktivitäten auf einfache Weise zu individuellen Profilen zusammengeführt werden können und eine dauerhafte Identifizierung somit möglich ist. Mit Hilfe von Zusatzinformationen, wie etwa Identifikationsdaten aus Nutzerkonten von Online-Shops, sozialen Netzwerken oder Maildiensten, Zukauf von Identifikationsdaten und Adressdaten, Zusatzwissen über die Aktivitäten, Gewohnheiten oder Vorlieben Betroffener und so weiter ist eine eindeutige Bestimmung von Nutzerinnen und Nutzern möglich. Die vereinfachten Möglichkeiten zur Profilbildung und Zusammenführung von Profilen erhöhen zudem das Risiko und verstärken die Auswirkungen krimineller Handlungen. Diese Technik bedarf spezieller Maßnahmen zum Schutz der Betroffenen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zu dieser Problematik eine Entschließung (siehe Ziffer 20.11 dieses Berichts) veröffentlicht.

Weiterhin soll die vom Arbeitskreis Technik veröffentlichte, aber nicht mehr dem Stand der Technik entsprechende Orientierungshilfe zum sicheren Löschen magnetischer Datenträger in einer gemeinsamen Arbeitsgruppe überarbeitet werden.

Im Bereich „Gesundheit“ hat eine Arbeitsgruppe des Arbeitskreises Technik eine Orientierungshilfe zu Krankenhausinformationssystemen erarbeitet (siehe Ziffer 7.1 dieses Berichts).

5. Inneres

5.1 Zensus 2011

Auch im Jahr 2011 beschäftigten wir uns wieder – wie schon die Jahre zuvor – mit dem Zensus 2011. Im Berichtsjahr wurden die Befragungen durchgeführt und die dafür erforderlichen Fragebögen an die Betroffenen versendet. Infolge dessen erhielten wir etliche Anfragen von Bürgerinnen und Bürgern, die wissen wollten, ob sie die ihnen zugesandten Bögen überhaupt ausfüllen müssen und ob einzelne Fragen unbeantwortet gelassen werden dürfen. Wir teilten den Befragten mit, dass es eine gesetzliche Verpflichtung gibt, alle Fragen, die nicht ausdrücklich als „frei-

willig“ gekennzeichnet sind, wahrheitsgemäß und vollständig zu beantworten. Wird der Auskunftspflicht nicht nachgekommen, drohen danach die Festsetzung eines Zwangsgeldes und die Verhängung eines Bußgeldes.

Verärgert waren zahlreiche Wohnungseigentümer und Gebäudeeigentümer darüber, dass sie mehrere Fragebögen zugesandt bekommen hatten, obwohl sie nur ein Objekt besitzen. Die Ursache für die Mehrfachversendungen bestand nach Angaben des Statistischen Landesamtes darin, dass im Vorfeld nicht alle Adressen der Befragten vollständig ermittelt werden konnten.

Im Mai des Berichtsjahres besichtigten wir die Erhebungsstelle in Bremerhaven. Dort fiel uns auf, dass kein Stahlschrank vorhanden war, in dem die ausgefüllten Fragebögen bis zu ihrer Abholung eingeschlossen werden können. Die Bögen wurden ohne gesonderten Schutz in der Erhebungsstelle aufbewahrt. Als Reaktion auf unsere Kritik wurden die Unterlagen schließlich in einem abschließbaren Behältnis gelagert. Die Anschaffung eines Stahlschrankes erledigte sich in der Folgezeit jedoch, da die Fragebögen inzwischen abgeholt worden waren.

Die in der Erhebungsstelle Bremerhaven eingesetzten Computer werden direkt durch das Statistische Landesamt administrativ betreut. Sie unterliegen somit den Regelungen des Datenschutzkonzeptes für den Zensus 2011.

Das Datenschutzkonzept des Statistischen Landesamtes wurde überarbeitet und von uns geprüft. Die im Datenschutzkonzept getroffenen Regelungen bedurften nur in einigen wenigen Punkten einer Klarstellung im Konzept selbst.

Im Rahmen der Ad-Hoc-Arbeitsgruppe Zensus 2011 der Landesbeauftragten für den Datenschutz und des Bundesbeauftragten für den Datenschutz wurden zahlreiche Fragen diskutiert, die beispielsweise die Erhebungsbeauftragten, das Einlesen der Fragebögen, Auskunftsansprüche und das Löschen von Zensusdaten betreffen.

5.2 Einrichtung eines automatisierten Direktzugriffs auf Melderegisterdaten für Kommunalbehörden ohne gesetzliche Grundlage

Die Einrichtung von automatisierten Direktzugriffen auf Melderegisterdaten für Kommunalbehörden beschäftigt uns schon seit geraumer Zeit. Inzwischen wurden vom Senator für Inneres und Sport für das automatisierte Abrufverfahren auf kommunaler Ebene das Stadtamt hinsichtlich staatsangehörigkeitsrechtlicher und namensrechtlicher Angelegenheiten, das Amt für Wohnungswesen, die Entsorgungsbetriebe Bremerhavens, der Umweltbetrieb Bremen sowie das Amt für Soziale Dienste freigeschaltet. Zwischen dem Senator für Inneres und Sport und uns besteht folgender Dissens: Während der Senator für Inneres und Sport in einem Auslegungserlass den nachgeordneten Meldebehörden mitteilte, dass eine Weitergabe der Meldedaten an öffentliche Stellen der Stadtgemeinde Bremen aufgrund der bestehenden Regelungen zulässig sei, halten wir eine gesonderte gesetzliche Grundlage für erforderlich. Es war geplant, im Zuge einer Überarbeitung der Meldedatenübermittlungsverordnung eine Lösung für die Streitfrage zu finden. Die Novellierung wurde jedoch vor dem Hintergrund eines neuen Bundesmeldegesetzes ausgesetzt. Der Gesetzentwurf enthält – anders als das Bremische Meldegesetz – eine ausdrückliche Regelung zur Einrichtung automatisierter Verfahren zur Datenübertragung an andere Stellen innerhalb einer Kommune. Danach müssen durch die Leitungen der Meldebehörden die abrufberechtigten Stellen sowie die erforderlichen technischen und organisatorischen Maßnahmen schriftlich festgelegt werden. Da es noch einige Zeit dauern wird, bis das neue Bundesmeldegesetz in Kraft tritt, wurde mit dem Senator für Inneres und Sport verabredet, dass in Vorwegnahme der geplanten Regelungen schon jetzt technische und organisatorische Maßnahmen zum Datenschutz von der Behördenleitung festgelegt werden. Zu diesem Zweck sollen uns vom Senator für Inneres und Sport die bereits vorhandenen Datenschutzkonzepte zur Verfügung gestellt werden.

5.3 Weitergabe von Meldedaten zu Zwecken der Wahlwerbung

Im Berichtsjahr erreichten uns einige Anrufe von Bürgerinnen und Bürgern, die sich darüber beschwerten, Werbung von politischen Parteien erhalten zu haben, und wissen wollten, was sie dagegen unternehmen können, wenn sie von Parteien angeschrieben werden. Einige der Betroffenen konnten sich nicht erklären, woher die Parteien ihre Adresse erhalten hätten.

Wir teilten den Betroffenen mit, dass es eine Vorschrift im Bremischen Meldegesetz gibt, die der Meldebehörde erlaubt, Parteien und Wählervereinigungen Auskunft aus dem Melderegister zu erteilen. Es dürfen dabei Auskünfte über Vornamen und Familiennamen, Doktorgrad und Anschrift von Personen erteilt werden, wenn die Personen wahlberechtigt oder stimmberechtigt sind und einer Gruppe angehören, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist. Durch diese Einschränkung soll verhindert werden, dass eine Partei oder Wählervereinigung Auskünfte über eine sehr große Anzahl von Personen aus dem Melderegister erhält. Die Geburtstage der Wahlberechtigten und Stimmberechtigten dürfen dabei nicht mitgeteilt werden. Die Verwendung der Daten durch die Parteien oder Wählervereinigungen ist streng zweckgebunden. Sie dürfen ausschließlich für Zwecke der Wahlwerbung oder Stimmwerbung verwendet werden. Spätestens einen Monat nach der Wahl oder Stimmabgabe sind die Daten von den betreffenden Parteien und Wählervereinigungen zu löschen. Die Löschung muss der Meldebehörde gegenüber schriftlich bestätigt werden.

Wer nicht möchte, dass die eigenen Daten zu Zwecken der Wahlwerbung und Stimmwerbung an Parteien oder Wählervereinigungen übermittelt werden, hat die Möglichkeit, der Weitergabe der Daten zu widersprechen. Dafür ausreichend ist ein formloser Antrag, der an die Meldebehörde gesendet werden muss. Ein Formular findet sich auf der Internetseite der Landesbeauftragten für Datenschutz und Informationsfreiheit unter www.datenschutz-bremen.de. Damit die Bürgerinnen und Bürger ihr Recht kennen, ist die Meldebehörde verpflichtet, bei Anmeldung und spätestens acht Monate vor jeder Wahl oder Stimmabgabe durch öffentliche Bekanntmachung auf das Widerspruchsrecht hinzuweisen.

5.4 Erteilung einer Auskunft aus dem Melderegister trotz Übermittlungssperre

Wir erhielten die Eingabe eines Bürgers, dessen Daten die Meldebehörde weitergeben wollte, obwohl für ihn im Melderegister aus Gründen des Personenschutzes eine Auskunftssperre eingetragen ist. Angefragt wurden die Informationen von einem Inkassounternehmen, welches wiederum von einer dritten Stelle mit der Einziehung einer offenen Forderung beim Petenten beauftragt worden war. Nach den gesetzlichen Regelungen kann die Erteilung einer Melderegisterauskunft selbst dann zulässig sein, wenn für die betreffende Person eine Übermittlungssperre eingetragen ist. Im konkreten Fall befürchtete der Betroffene jedoch, dass seine Daten durch die Herausgabe in unbefugte Hände gelangen und er dadurch gefährdet werden könnte. Die Meldebehörde gab dem Petenten Gelegenheit, sich zu der beabsichtigten Auskunftserteilung zu äußern. Von der Gelegenheit machte der Betroffene Gebrauch. Die Meldebehörde kam daraufhin zu dem Ergebnis, dass dem Petenten durch die Melderegisterauskunft keine Gefahr drohe. Dennoch sollte vor Erteilung der Melderegisterauskunft abgewartet werden, ob der Streit um die zugrundeliegende Forderung nicht kurzfristig geklärt werden könne und damit eine Melderegisterauskunft überflüssig werde.

Wir vertraten im Gegensatz zur Meldebehörde die Auffassung, dass eine Datenübermittlung an das Inkassounternehmen unzulässig ist, da eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen nicht – wie es das Gesetz fordert – ausgeschlossen werden könne. Zumindest hatte die Meldebehörde nach unserer Auffassung nicht ausreichend dargelegt, warum eine entsprechende Gefahr auszuschließen sei. Die Meldebehörde befürchtete hingegen, dass sich eine Person mit der Eintragung einer Auskunftssperre der Verfolgung und Durchsetzung berechtigter zivilrechtlicher Forderungen entziehen könne. Die Frage wurde von der Meldebehörde zur Klärung dem Senator für Inneres und Sport vorgelegt. Dieser teilte unsere Bedenken nicht. Der Petent teilte uns in der Zwischenzeit mit, dass er an die Meldebehörde ein Schreiben gesendet habe, aus welchem sich die Erledigung der zugrundeliegenden Forderung ergebe. Dennoch erteilte die Meldebehörde gegenüber dem Inkassounternehmen die gewünschte Melderegisterauskunft. Das vorangegangene Schreiben des Petenten war in der Meldebehörde bei der Entscheidung über die Erteilung der Melderegisterauskunft aufgrund eines Büroversehens unberücksichtigt geblieben. Wir forderten daraufhin die Meldebehörde auf, technische und organisatorische Vorkehrungen zu treffen, um solche Fehler in Zukunft zu vermeiden. Die Meldebehörde lehnte unserer Forderung mit der Begründung ab, dass es sich ausschließlich um ein individuelles Versehen gehandelt habe und deshalb keine Veranlassung bestehe, bewährte organisatorische Regelungen zur Behandlung von Posteingängen zu verändern.

5.5 Datenschutzflyer der Polizei Bremen

Die Polizei Bremen gibt aktuell einen Datenschutzflyer heraus, der sich mit Fragen beschäftigt, die häufig von den Bürgerinnen und Bürgern gestellt werden. Zum Beispiel wird in dieser Broschüre darüber informiert, dass es datenschutzrechtlich zulässig ist, dass bei der Wahl der Notrufnummer 110 das Gespräch aufgezeichnet wird. Daneben werden Themen wie Strafanzeigen, allgemeine Verkehrskontrollen, Frontalaufnahmen beim „Blitzen", Videoaufzeichnungen von Demonstrationen, Fotos und Fingerabdrücke aus erkennungsdienstlichen Behandlungen, Kriminalakten und das Auskunftsrecht von Bürgerinnen und Bürgern behandelt.

Wir begrüßen es, dass sich der Datenschutzbeauftragte der Polizei Bremen nunmehr im Internet unter www.polizei.bremen.de präsentiert und dort diesen Datenschutzflyer zum Herunterladen zur Verfügung stellt.

5.6 Kontrollbesuch bei der Polizei Bremen

Die Polizei Bremen verfügt über ein Intranet, das sogenannte Intrapol, welches diverse personenbezogene Informationen wie zum Beispiel Intensivtäterliste, Ereignismeldungen, Platzverweise, Wohnungsverweisungen, Firmenliste, Gaststättenliste und Beförderungsverbote der Bremer Straßenbahn Aktiengesellschaft (BSAG) enthält. Aus diesem Grunde haben wir uns die Berechtigungsstruktur betreffend der Zugriffe auf diese unterschiedlichen personenbezogenen Daten angesehen. Bei unserer Kontrolle fiel auf, dass die Berechtigungsstruktur hinsichtlich der Zugriffe auf die personenbezogenen Daten im Intranet wenig differenziert ist, und hauptsächlich zwischen Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten auf der einen und tariflich Angestellten auf der anderen Seite unterschieden wird, was zu unverhältnismäßigen Eingriffen in das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger führt. Selbst diese grobe Einteilung wurde allerdings nicht konsequent durchgehalten und wir konnten die theoretische Möglichkeit der Einsichtnahme beziehungsweise der Eingabe von personenbezogenen Daten durch die Berechtigungsgruppe Tarifpersonal feststellen. Beispiele dafür sind die Anwendung „Wohnungsverweise", das Sperrsystem „KUNO" (Kriminalitätsbekämpfung im unbaren Zahlungsverkehr unter Nutzung nichtpolizeilicher Organisationsstrukturen) und der Bereich „Fahndung". In einer Vielzahl der Anwendungen, die personenbezogene Daten beinhalten, gab es keine Verfahrensbeschreibungen, die das Bremische Datenschutzgesetz voraussetzt. Somit ist beispielsweise nicht feststellbar, ob die Kontrollziele nach dem Bremischen Datenschutzgesetz wie beispielsweise die Eingabekontrollen gewährleistet sind. Wir haben die Polizei Bremen aufgefordert, das technische Berechtigungskonzept zu erstellen, die Berechtigungen anzupassen, uns die fehlenden Verfahrensbeschreibungen zu übersenden und das Ergebnis der Vorabkontrolle des polizeilichen Datenschutzbeauftragten mitzuteilen. Eine Stellungnahme der Polizei Bremen steht derzeit noch aus.

5.7 Sichere Kommunikation zwischen der Polizei Bremen und der Staatsanwaltschaft Bremen

Grundsätzlich taucht in unserer datenschutzrechtlichen Tätigkeit die Frage der sicheren Kommunikation immer wieder auf. Mit Blick auf das Projekt „Stopp der Jugendgewalt" ist diese Frage aktuell von datenschutzrechtlicher Bedeutung bei der Kommunikation zwischen der Polizei Bremen und der Staatsanwaltschaft Bremen. Sofern über den elektronischen Übertragungsweg der E-Mail personenbezogene Daten zwischen diesen beiden Behörden ausgetauscht werden, halten wir eine Verschlüsselung dieser personenbezogenen Daten für erforderlich. Unter personenbezogene Daten werden beispielsweise die persönlichen Daten oder nicht öffentlich zugängliche, polizeiinterne Fahndungsdaten einschließlich Fotoaufnahmen von jugendlichen Straftäterinnen und Straftätern verstanden. Diese personenbezogenen Daten sind äußerst sensibel und vor einer unbefugten Kenntnisnahme Dritter zu schützen.

Für diese Daten müssen Vertraulichkeit, Integrität, Authentizität der Daten und der Kommunikationspartner sowie in Abhängigkeit von der Weiterverwendung auch Nicht-Abstreitbarkeit der Herkunft und des Erhalts gewährleistet werden. Eine symmetrische Verschlüsselung, wie zunächst von der Polizei Bremen angedacht, leistet diese Anforderungen nicht.

Der Einsatz eines geeigneten Verfahrens mit asymmetrischer Verschlüsselung bei dem nur der rechtmäßige Empfänger in der Lage ist, durch seinen privaten Schlüssel

die Nachricht zu entschlüsseln, die zuvor mit seinem öffentlichen Schlüssel verschlüsselt worden ist, kann den Anforderungen an die elektronische Übermittlung von Dokumenten mit dem Schutzbedarf „hoch“ gerecht werden. Durch Verwendung von Signaturen und Zertifikaten können Integrität, Authentizität und Nicht-Abstreitbarkeit gewährleistet werden.

Wir haben daher die Polizei Bremen und die Staatsanwaltschaft Bremen aufgefordert, eine Lösung zu implementieren, welche das geforderte Sicherheitsniveau gewährleistet.

5.8 Vortrag über polizeiliche Tätigkeiten im Internet

Das Thema „Soziale Netzwerke“ beschäftigt uns aus datenschutzrechtlicher Sicht immer mehr. Aber auch die Polizei hat dieses Feld als Informationsquelle für sich entdeckt. Aus diesem Grunde haben wir im Rahmen des Wahlpflichtmoduls „Internet und Soziale Netzwerke“ des Instituts für Polizeiforschung und Sicherheitsforschung an der Hochschule für Öffentliche Verwaltung einen Vortrag über Möglichkeiten polizeilicher Ermittlungen im Internet, insbesondere im Hinblick auf die sozialen Netzwerke, und die datenschutzrechtlichen Grenzen der polizeilichen Tätigkeit im Internet gehalten, der auf unserer Internetseite unter www.datenschutz.bremen.de zum Herunterladen zur Verfügung gestellt wird. Diese Thematik beinhaltet neben den Übermittlungsbefugnissen von personenbezogenen Daten durch die Betreiber der sozialen Netzwerke auch die Erhebungsbefugnisse dieser Daten durch die Polizei und allgemein die polizeilichen Ermittlungen in einem sozialen Netzwerk unter Zuhilfenahme einer Legende oder einem offen erkennbaren Polizei-Account (Konto).

5.9 Datenschutzkonzepte der Ortspolizeibehörde Bremerhaven

Die Ortspolizeibehörde Bremerhaven wird ein neues System für die Einsatzleitstelle einführen. Insbesondere spielen die Speicherung von Einsatzdaten und Notrufdaten sowie von GPS-Daten eine wichtige Rolle. Die Ortspolizeibehörde Bremerhaven hat uns vor Einführung dieses Systems beteiligt.

Die umgangssprachliche Abkürzung „GPS“ steht für „Global Positioning System“ und stellt ein satellitengestütztes System zur weltweiten Zeitmessung und Positionsbestimmung dar.

Wir erachten bezüglich der Notrufgespräche eine Speicherdauer von einem Monat und für die Einsatzdaten grundsätzlich eine Speicherdauer von sechs Monaten als zulässig, wobei ausnahmsweise bei Ermittlungsverfahren und strafrechtlichen Gerichtsverfahren die Notrufdaten und Einsatzdaten zu Beweiszwecken nach der Strafprozessordnung länger aufbewahrt werden dürfen. Die Aufbewahrungsdauer der Einsatzdaten von sechs Monaten reicht der Ortspolizeibehörde nicht aus. Die Einsatzdaten müssen aus ihrer Sicht bei der Polizei zwei Jahre lang gespeichert werden. Hier besteht ein Dissens. Wir haben die Ortspolizeibehörde Bremerhaven darauf hingewiesen, dass eine Verfahrensbeschreibung und ein Datenschutzkonzept zu erstellen sind und der behördliche Datenschutzbeauftragte die Vorabkontrolle vorzunehmen hat. In diesem Zusammenhang haben wir die Polizeibehörde Bremerhaven auch bezüglich der technischen und rechtlichen Voraussetzungen zur Durchführung einer Fernwartung beraten.

In diesem Zusammenhang mit der Einführung einer neuen Software bei der Einsatzleitstelle eröffnet sich durch die Veränderung des Funk-Notruf-Abfrage-Systems die Möglichkeit für die Ortspolizeibehörde Bremerhaven, bei der Polizei eingehende Notrufe an die Feuerwehr weiterzuleiten, wobei die Polizei weiterhin das Gespräch am Telefon mithören kann. Auch hinsichtlich des Einsatzes dieser Funktion bestand Beratungsbedarf für die Ortspolizeibehörde Bremerhaven. Die Weiterleitung der Anrufe durch die Ortspolizeibehörde Bremerhaven an die Feuerwehr Bremerhaven und das Mithören der Ortspolizeibehörde Bremerhaven sind unseres Erachtens unter bestimmten Voraussetzungen zulässig. Wir haben die Ortspolizeibehörde Bremerhaven darauf hingewiesen, dass sie dafür Sorge zu tragen hat, dass diese Voraussetzungen erfüllt werden. Weiter wurde die Ortspolizeibehörde Bremerhaven zur funktionalen Erweiterung „Volltextrecherche“ in ihrem Einsatzsystem „RevierS“ beraten. Das Bremische Polizeigesetz steht dem entgegen. Insoweit ist die Volltextrecherche unzulässig.

5.10 Datenschutzkonzepte beim Senator für Inneres und Sport sowie bei der Zentralen Antikorruptionsstelle

Der Senator für Inneres und Sport hat nunmehr ein Rahmendatenschutzkonzept zur allgemeinen Infrastruktur vorgelegt. Insbesondere spielen Themen wie Zugangsberechtigungen und Zugriffsberechtigungen, Protokollierungen und die Verschlüsselung von personenbezogenen Daten auf dem Übertragungsweg eine datenschutzrechtlich wichtige Rolle in der allgemeinen Infrastruktur des Senators für Inneres und Sport. Sowohl die Abschottung der Infrastruktur gegenüber dem Bremer Verwaltungsnetz (BVN) und dem Internet, Regelungen zur Vergabe von Berechtigungen sowie eine Dienstanweisung für den Umgang mit Notebooks sind datenschutzrechtliche Anforderungen und somit durch das Rahmendatenschutzkonzept zu beschreiben. Das Informationstechnologie-Betriebskonzept, auf welches das Rahmendatenschutzkonzept an einigen Stellen verweist, steht derzeit noch aus. Wir haben eine vorläufige datenschutzrechtliche Beurteilung abgegeben und befinden uns derzeit in einem gegenseitigen Austausch.

Die Zentrale Antikorruptionsstelle, die auch dem Rahmendatenschutzkonzept des Senators für Inneres und Sport unterfällt, benutzt eine eigene automatisierte Datenverarbeitung, welche die Anforderungen des Bremischen Datenschutzgesetzes einzuhalten hat. Insbesondere sind hier die Protokollierung und die Zugriffsberechtigungen von datenschutzrechtlichem Interesse. Die Frage, ob hier bei der Speicherung von Word-Dateien eine automatisierte Datenverarbeitung vorliegt, stellt sich unseres Erachtens nicht. Nach dem Bremischen Datenschutzgesetz wird unter automatisierter Datenverarbeitung die Verarbeitung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen verstanden. Bei der Speicherung von personenbezogenen Daten durch sogenannte Standardprodukte für Textverarbeitung oder Tabellenkalkulation handelt es sich somit um eine automatisierte Sammlung personenbezogener Daten, für deren Schutz die technischen und organisatorischen Maßnahmen nach dem Bremischen Datenschutzgesetz festzulegen sind. Auch der Einsatz mobiler Speicher wie zum Beispiel Notebooks birgt Datenschutzrisiken, die besonders zu beachten sind. Unklarheiten gibt es derzeit noch bezüglich der von uns geforderten verschlüsselten Speicherung der Daten, der fehlenden Eingabekontrolle und der von uns nicht akzeptierten lokalen Speicherung von Daten auf Arbeitsstationen. Hier stellen wir besondere Anforderungen, da die Daten einem besonders hohen Schutzniveau unterliegen. Die unsachgemäße Handhabung dieser besonders sensiblen personenbezogenen Daten können die Betroffenen in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen erheblich beeinträchtigen. Der Zentralen Antikorruptionsstelle liegt unsere datenschutzrechtliche Beurteilung vor. Wir befinden uns aktuell in einem Abstimmungsprozess.

5.11 Datenschutzkonzepte beim Stadtamt Bremen

Aufgrund der Vielfältigkeit der datenschutzrechtlichen Themen im Stadtamt Bremen wurde die Zusammenarbeit derart gestaltet, dass quartalsweise Gespräche zu den verschiedenen Datenschutzkonzepten des Stadtamtes stattfinden. Folgende Themen weisen noch immer datenschutzrechtliche Aktualität auf: Rahmendatenschutzkonzept, Informationstechnologie-Betriebskonzept, AusländerDatenVerwaltungsSystem und InformationsSystem (ADVIS), Fundinfo, Hess Zahlungssystem, Informationstechnologie-Verfahren IKONIZER zur Verwaltung der Schließanlage, Marktverwaltung, Mobiler Bürgerservice und Waffenverwaltung (vergleiche 33. Jahresbericht, Ziffern 5.9 und 5.16). Wir begrüßen die enge fachliche und kooperative Zusammenarbeit mit dem Stadtamt. Allerdings erwarten wir nun auch die zügige Umsetzung der mit uns abgestimmten Maßnahmen.

5.12 Bremisches Spielhallengesetz

Die Vorüberlegungen zum endgültigen Gesetzentwurf eines Bremischen Spielhallengesetzes sahen Ende März 2011 aus datenschutzrechtlicher Sicht nur eine Alterskontrolle mittels Identifizierungsnachweises vor. Insoweit gaben wir eine datenschutzrechtliche Stellungnahme ab. Eine Spielersperre war aufgrund der Sachnähe zum Gewerberecht nicht Gegenstand dieser Vorüberlegungen. In einem Dringlichkeitsantrag der Fraktionen Sozialdemokratische Partei Deutschlands (SPD) und Bündnis 90/Die Grünen wurde dann jedoch die Spielersperre in den Gesetzentwurf aufgenommen. Das Bremische Spielhallengesetz gilt seit dem 20. Mai 2011. Diese

Bestimmung über die Spielersperre hat datenschutzrechtliche Konsequenzen für die Spielhallen, auf die wir im Folgenden hinweisen möchten.

Grundsätzlich haben die Spielhallen, also auch die Spielcasinos, die dem Bremischen Spielhallengesetz unterfallen, darauf zu achten, dass die Vorgaben des Bundesdatenschutzgesetzes, auch die der technischen und organisatorischen Maßnahmen zum Datenschutz, eingehalten werden.

Bei der Überprüfung der Identität nach dem neuen Bremischen Spielhallengesetz ist zu beachten, dass Spielhallen, die dem Gesetz unterfallen, durch ihr Personal sicherstellen müssen, dass Gäste, die eine Spielhalle betreten und spielen wollen, ihre amtlichen Ausweise vorlegen. Dies dient der Einhaltung der altersbeschränkten Zutrittskontrolle. Dies bedeutet, dass beispielsweise die Anfertigung von Ausweiskopien, das elektronische Auslesen des amtlichen Ausweises oder das Erstellen einer tagesaktuellen Liste mit allen Gästen oder eine sonstige Verarbeitung von Namen oder anderen Daten, die aus dem amtlichen Ausweis ersichtlich sind, wie zum Beispiel die Adresse, untersagt sind, weil diese Maßnahmen nicht erforderlich sind, um die Altersbeschränkung zu kontrollieren. In der Begründung zum Bremischen Spielhallengesetz wird dazu ausgeführt, dass eine dauerhafte Speicherung der persönlichen Daten bei der Identitätsüberprüfung weder erforderlich noch zulässig ist.

Weiter ist eine Spielersperrliste zu führen. Hinsichtlich der Spielersperrliste ist zu differenzieren zwischen dem Abgleich dieses Dokuments mit dem vorgezeigten amtlichen Ausweis beim Eintritt in eine Spielhalle einerseits und dem Führen der Liste und der Aufnahme von Spielerinnen und Spielern in sie (bei freiwilliger Selbstsperre) andererseits. Die Aufgaben des Abgleichs der Spielersperrliste und der Inaugenscheinnahme des amtlichen Ausweises beim Betreten des Spielcasinos sollten in einer Person vereint sein, damit so wenig Personen wie möglich und soviel Personen wie erforderlich die amtlichen Ausweise und die Liste einsehen. Beim Abgleich der personenbezogenen Daten des amtlichen Ausweises mit der Spielersperrliste ist darauf zu achten, dass nur die von der Spielhalle mit der Funktion des Abgleichs der Spielersperrliste beauftragte Person die Liste einsehen kann (Zugriffskontrolle). Unbefugte Personen wie zum Beispiel andere Mitarbeiterinnen und Mitarbeiter oder auch Gäste dürfen die Spielersperrliste nicht einsehen. Es obliegt der Spielhalle, dies sicherzustellen. Das Bremische Spielhallengesetz enthält keine Vorgaben, ob die Spielersperrliste in physischer oder elektronischer Form geführt werden soll (vergleiche Drucksache der Bremischen Bürgerschaft 17/1736 vom 5. April 2011, Seite 9). Die Spielersperrliste hat unabhängig von der Form nur die zur Identifikation erforderlichen personenbezogenen Daten wie Name, Vorname, Geburtsdatum und Geburtsort zu enthalten. Hier ist eine Einwilligung der Betroffenen für die Datenerhebung, Datenspeicherung und Datennutzung durch die Spielhalle im Rahmen der freiwilligen Spielersperre erforderlich. Die Spielersperrliste ist gegen die Kenntnisnahme unbefugter Dritter zu schützen und aktuell zu halten, sodass nach Ende der Spielersperre die personenbezogenen Daten in der Liste zu löschen sind. Grundsätzliche wichtige Hinweise zum sicheren Löschen und Vernichten von Daten können Sie auf unserer Internetseite www.datenschutz.bremen.de abrufen. Unter dem Unterpunkt „Technik“ findet sich das Dokument „Verräterische Spuren auf Festplatten – Hinweis zum sicheren Löschen von Daten“. Unter dem Unterpunkt „Hilfestellungen“ befindet sich das Dokument „Entwicklung eines Konzeptes zur Löschung und Datenträgervernichtung durch Behörden und Unternehmen“.

Außerdem stellt das Gesetz datenschutzrechtliche Anforderungen an den Umgang mit den Unterlagen bei einer freiwilligen Selbstsperre in einer Spielhalle. Spielerinnen und Spieler können sich grundsätzlich selbst sperren lassen. Wenn das schriftliche Sperrverlangen persönlich überbracht wird, dann reicht die Vorlage des Ausweisdokuments bei Abgabe des Sperrverlangens zur eindeutigen Identifizierung aus. Wenn Spielerinnen oder Spieler die freiwillige Spielersperre schriftlich verlangen, dann sollten sie allein zur eindeutigen Identifizierung auf dem Postwege eine Kopie des amtlichen Ausweises zusammen mit dem Sperrgesuch einreichen. Zur Frage der Ausweiskopien im Rahmen der Identitätskontrolle bei freiwilligen Selbstsperren möchten wir darauf hinweisen, dass die Spielerinnen und Spieler die Kopien der amtlichen Ausweise dahingehend schwärzen können, dass Daten, die nicht zu Identifizierungszwecken benötigt werden, auch der jeweiligen Spielhalle nicht mitgeteilt werden müssen. Das Schwärzen gilt insbesondere für sämtliche auf dem Ausweis befindlichen Nummern sowie Nationalität, Augenfarbe und Größe. Für den Fall, dass Spielerinnen oder Spieler von der Möglichkeit des Schwärzens der

Ausweiskopien keinen Gebrauch machen, möchten wir darauf hinweisen, dass Ausweisdaten wie zum Beispiel Ausweisnummer oder Augenfarbe nicht gespeichert werden dürfen. Weiter möchten wir darauf hinweisen, dass die (eventuell geschwärzten) Ausweiskopien zu vernichten sind, sobald sie nicht mehr benötigt werden und damit für das Führen der Spielersperrliste nicht mehr erforderlich sind. Dies ist in der Regel sofort nach dem Abgleich des Spielersperrgesuchs mit der Ausweiskopie zum Zwecke der Identifizierung der Fall. Sämtliche Unterlagen der freiwilligen Selbstsperre sind vor unbefugter Kenntnisnahme Dritter geschützt aufzubewahren.

Wir forderten die Spielhallen in Bremen und Bremerhaven hiermit auf, diese datenschutzrechtlichen Anforderungen in der Praxis zu beachten.

5.13 Datenschutz in Sportvereinen

Wir beraten gern Sportvereine in datenschutzrechtlichen Fragen (vergleiche 33. Jahresbericht, Ziffer 5.14) wie zum Beispiel der Ausgestaltung von Einwilligungserklärungen, die die Grundlage für die Veröffentlichung von Fotoaufnahmen von Vereinsmitgliedern im Internet bilden. Auf den Internetseiten von Sportvereinen finden sich häufig Fotoaufnahmen von einzelnen Sportlerinnen und Sportlern oder auch einer kleinen Gruppe von Vereinsmitgliedern. Für die Veröffentlichung von Fotoaufnahmen von Sportlerinnen und Sportlern im Internet ist eine Einwilligung der jeweiligen Person erforderlich, die die Voraussetzungen des Bundesdatenschutzgesetzes erfüllt. Ohne eine solche Einwilligungserklärung des Vereinsmitglieds ist eine Veröffentlichung im Internet nicht zulässig. Wir möchten an dieser Stelle darauf aufmerksam machen, dass nach Widerruf des Einverständnisses und nach der Löschung der Fotoaufnahmen von der Internetseite des Sportvereins eine weitere Speicherung im Internet zum Beispiel bei Suchmaschinen möglich ist.

Weiter beraten wir Sportvereine hinsichtlich der Vorlage von erweiterten Führungszeugnissen. Aus Minderjährigenschutzgründen können die Sportvereine Übungsleiterinnen und Übungsleiter, die beruflich oder ehrenamtlich Minderjährige beaufsichtigen oder betreuen, auffordern, erweiterte Führungszeugnisse gemäß dem Bundeszentralregistergesetz zu beantragen und dem Sportverein vorzulegen.

Das erweiterte Führungszeugnis enthält den die Antrag stellende, über 14-jährige Personen betreffenden Inhalt des Zentralregisters. Es beinhaltet über das einfache Führungszeugnis hinaus eine Auskunft über das Kindeswohl gefährdende Delikte und ist umfassend. Aus diesem Grunde kann es unter Umständen vorkommen, dass zum Beispiel eine für die Betreuung und die Arbeit mit Minderjährigen irrelevante Verurteilung wegen Betrugs aus dem erweiterten Führungszeugnis ersichtlich sein kann. Die Verwendung von Inhalten des erweiterten Führungszeugnisses ist auf den für die Beantragung maßgeblichen Zweck des Minderjährigenschutzes begrenzt. Es lässt sich in der Praxis nicht ausschließen, dass der Sportverein bei Vorlage eines erweiterten Führungszeugnisses Kenntnis von einer für den Minderjährigenschutz bedeutungslosen Verurteilung erhält. Eine Nutzung, Speicherung oder Weitergabe dieser Information durch den zur Einsichtnahme in das erweiterte Führungszeugnis Berechtigten zum Beispiel wegen einer etwaigen Tätigkeit der Übungsleiterin beziehungsweise des Übungsleiters als Kassenwart im Sportverein ist datenschutzrechtlich aber unzulässig.

Nach dem Bundeszentralregistergesetz wird das erweiterte Führungszeugnis der Antrag stellenden Person übersandt. Insofern obliegt es der Antrag stellenden Person zu entscheiden, ob sie das erweiterte Führungszeugnis dem Sportverein vorlegen möchte oder nicht. Das erweiterte Führungszeugnis ist der Antrag stellenden Person, also der Übungsleiterin oder dem Übungsleiter, nach Vorlage beim Sportverein zurückzugeben. Eine Kopie, die möglicherweise der Sportverein besitzen möchte, darf aus datenschutzrechtlicher Sicht mangels Geeignetheit und Erforderlichkeit nicht angefertigt werden.

Wir gehen davon aus, dass die Sportvereine und der Senator für Inneres und Sport diese datenschutzrechtlichen Aspekte bei ihrer Tätigkeit berücksichtigen.

5.14 Bericht aus dem Arbeitskreis Sicherheit

Auch in diesem Jahr tagte wieder der Arbeitskreis Sicherheit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Er dient dem Erfahrungsaustausch und Informationsaustausch. Themen waren unter anderem:

— die Funkzellenabfrage (vergleiche die Entschließung vom 27. Juli 2011, Ziffer 20.7 dieses Berichts und die Entschließung vom 29. September 2011, Ziffer 20.13 dieses Berichts),

— die Telekommunikationsüberwachung (vergleiche die Entschließung vom 17. März 2011, Ziffer 20.4 dieses Berichts) und das Telekommunikationsüberwachungszentrum Nord,

— die polizeiliche Videoüberwachung in den verschiedenen Bundesländern,

— die Polizei im Internet (vergleiche Ziffer 5.8 dieses Berichts und die Entschließung vom 29. September 2011, Ziffer 20.12 dieses Berichts, vergleiche 33. Jahresbericht, Ziffer 5.18),

— Zuverlässigkeitsüberprüfungen bei Großveranstaltungen,

— die Ahndungspraxis bei unbefugten Abrufen aus polizeilichen Informationssystemen durch Polizeibeamte,

— Ganzkörperscanner an Flughäfen,

— das Projekt „Analyse von Personenbewegungen an Flughäfen mittels zeitlich rückwärtsgerichteter und vorwärtsgerichteter Videodatenströme“ unter dem Blickwinkel der Berücksichtigung des Datenschutzes bei öffentlich geförderten Forschungsvorhaben,

— das nachrichtendienstliche Informationssystem in Bezug auf das Hosting der Amtsdatei des Verfassungsschutzes (vergleiche 33. Jahresbericht, Ziffer 5.17) und der Kernbereichsschutz im Verfassungsschutz,

— die Evaluation des Terrorismusbekämpfungsergänzungsgesetzes und zehn Jahre Antiterrorgesetze (vergleiche die Entschließung vom 29. September 2011, Ziffer 20.8 dieses Berichts) sowie

— die Einführung eines europäischen Systems zur Verarbeitung von Flugpassagierdaten (vergleiche die Entschließung vom 17. März 2011, Ziffer 20.5 dieses Berichts).

6. Justiz

6.1 Adressangabe von Zeugen in Strafverfahren

Es erreichen uns immer wieder Fragen von Bürgerinnen und Bürgern als Zeuginnen und Zeugen in Strafverfahren, inwieweit die eigene Anschrift aus der Ermittlungsakte beziehungsweise Strafverfahrensakte hervorgehen muss. Insbesondere bei Stalkingfällen wird als Befürchtung vorgetragen, dass das Stalking durch die Aufnahme der Wohnadresse von Zeuginnen und Zeugen in die Akte durch die Akteneinsicht der Verteidigerin oder des Verteidigers und damit durch die Weitergabe der Information das Stalking vom Arbeitsumfeld auf das Wohnumfeld beziehungsweise vom virtuellen Internet auf die tatsächliche Welt ausgedehnt wird.

Durch das Zweite Opferrechtsreformgesetz kam es zu Änderungen in der Strafprozessordnung mit Wirkung zum 1. Oktober 2009. Danach sind Zeuginnen und Zeugen als Beweismittel nunmehr mit ihrem Wohnort oder Aufenthaltsort in der Anklageschrift anzugeben. Allerdings bedarf es dabei nicht der Angabe der vollständigen Anschrift. Dies liegt im Ermessen der die Anklage verfassenden Staatsanwaltschaft. Zur Erfüllung des von der Anklageschrift zu befriedigenden Informationsinteresses der Angeklagten oder des Angeklagten sollte – wie der Gesetzgeber nunmehr klar zum Ausdruck gebracht hat – grundsätzlich die bloße Angabe des Wohnortes oder Aufenthaltsortes ausreichen. Wir haben festgestellt, dass seitens der Staatsanwaltschaft Bremen diese Norm in der Praxis eingehalten wird und in der Anklageschrift nur der Vorname und Zuname sowie der Wohnort aufgeführt werden.

Allerdings kam es auch zu Beschwerden darüber, dass die vollständige Adresse häufig bereits in der Ermittlungsakte bei einer Zeugenvernehmung durch die Polizei vorhanden ist, so dass später bei Akteneinsicht der Verteidigerin oder des Verteidigers die vollständige Anschrift von Zeuginnen und Zeugen preisgegeben wird. Bei der Vernehmung einer Zeugin oder eines Zeugen durch die Polizei gilt grundsätzlich, dass die Vernehmung damit beginnt, dass die Zeugin oder der Zeuge über Vornamen, Nachnamen, Geburtsnamen, Alter, Beruf und Wohnort befragt

wird. Einer Zeugin oder einem Zeugen soll nach der Strafprozessordnung gestattet werden, statt des Wohnortes ihren beziehungsweise seinen Geschäftsort oder Dienstort oder eine andere ladungsfähige Anschrift anzugeben, wenn ein begründeter Anlass zu der Besorgnis besteht, dass durch die Angabe des Wohnortes Rechtsgüter der Zeugin oder des Zeugen oder einer anderen Person gefährdet werden oder dass auf die Zeugin oder den Zeugen oder eine andere Person in unlauterer Weise eingewirkt werden wird. Bei entsprechenden Anhaltspunkten für eine solche Besorgnis der Gefährdung sind Zeuginnen und Zeugen darauf hinzuweisen, dass sie statt des Wohnortes ihren Geschäftsort oder Dienstort oder eine andere ladungsfähige Anschrift angeben können. Die Polizei soll die Zeugin oder den Zeugen bei der Benennung einer ladungsfähigen Anschrift unterstützen. Die Unterlagen, die die Feststellung des Wohnortes oder der Identität der Betreffenden gewährleisten, sind bei der Staatsanwaltschaft zu verwahren. Zu den Akten sind sie erst zu nehmen, wenn die Besorgnis der Gefährdung entfällt. An diese Bestimmungen der Strafprozessordnung haben sich sowohl die Staatsanwaltschaft als auch die Polizei nach Abschluss der Zeugenvernehmung zu halten. Soweit der Zeugin oder dem Zeugen gestattet wurde, Daten nicht anzugeben, ist bei Auskünften aus und Einsichtnahmen in Akten sicherzustellen, dass diese Daten anderen Personen wie zum Beispiel der Verteidigerin oder dem Verteidiger nicht bekannt werden, es sei denn, dass eine solche Gefährdung ausgeschlossen erscheint. Wir gehen davon aus, dass bei Stalkingfällen grundsätzlich die Besorgnis besteht, dass durch die Angabe des Wohnortes Rechtsgüter der Zeugin oder des Zeugen oder einer anderen Person gefährdet werden oder dass auf Zeuginnen und Zeugen oder eine andere Person in unlauterer Weise eingewirkt werden wird. Insofern fordern wir die Staatsanwaltschaft Bremen und die Polizei in solchen Stalkingfällen auf, über diese Bestimmungen in der Strafprozessordnung frühzeitig aufzuklären und die Zeugin oder den Zeugen bereits bei der Aufnahme der Strafanzeige darauf hinzuweisen, statt des Wohnortes ihren beziehungsweise seinen Geschäftsort oder Dienstort oder eine andere ladungsfähige Anschrift anzugeben und diese Betreffenden bei der Benennung einer ladungsfähigen Anschrift zu unterstützen, um die Opferschutzvorschriften und Zeugenschutzvorschriften der Strafprozessordnung nicht zu unterlaufen.

6.2 Bericht aus dem Arbeitskreis Justiz

Auch in diesem Jahr tagte wieder der Arbeitskreis Justiz der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Der Arbeitskreis dient dem Erfahrungsaustausch und Informationsaustausch. Themen waren unter anderem:

— Staatstrojaner und Quellentelekommunikationsüberwachung,

— Funkzellenabfrage (vergleiche Entschließung vom 27. Juli 2011, Ziffer 20.7 dieses Berichts und Entschließung vom 29. September 2011, Ziffer 20.13 dieses Berichts),

— elektronische Aufenthaltsüberwachung,

— elektronisches Schuldnerverzeichnis,

— elektronisches Grundbuch,

— DNA-Analyse nach der Strafprozessordnung,

— Ermittlungen in sozialen Netzwerken (siehe Ziffer 5.8 dieses Berichts und Entschließung vom 29. September 2011, Ziffer 20.12 dieses Berichts; vergleiche 33. Jahresbericht, Ziffer 5.18) und

— Europäische Ermittlungsanordnung.

Besondere Bedeutung kommt dem sogenannten Trojaner bei der staatsanwaltlichen Überwachung der Telekommunikation zu. Unter dem Trojaner wird eine Software verstanden, die eigens für die einzelne polizeiliche Überwachungsmaßnahme der Telekommunikation entwickelt wurde. In Bremen gab es bisher einen Fall einer solchen Telekommunikationsüberwachung im Jahr 2007, der derzeit von uns geprüft wird.

7. Gesundheit und Soziales

7.1 Orientierungshilfe Krankenhausinformationssysteme

Im Juni 2009 informierte der Hamburgische Datenschutzbeauftragte über die Erarbeitung von vierzig normativen Eckpunkten für die Zugriffe auf elektronische Pa-

tientenakten in Krankenhäusern im Dialog mit Hamburger Krankenhäusern. Anlass war die Feststellung von erheblichen Defiziten bei den Zugriffsregelungen auf Patientendaten in Krankenhäusern gewesen. Im fachlichen Austausch der Datenschutzbeauftragten wurde festgestellt, dass diese Probleme bereits in verschiedenen Ländern bekannt geworden waren. Aus diesem Grunde wurde von dem Arbeitskreis Gesundheit und Soziales und dem Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Unterarbeitsgruppe Krankenhausinformationssysteme eingesetzt, die in Zusammenarbeit mit dem Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und dem Datenschutzbeauftragten der norddeutschen Bistümer der Katholischen Kirche und in der Diskussion mit Herstellern und Betreibern eine Orientierungshilfe für rechtliche und technische Anforderungen an einen datenschutzkonformen Betrieb von Krankenhausinformationssystemen erarbeitete. Die Orientierungshilfe wurde im März 2011 von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und im Mai 2011 vom Düsseldorfer Kreis verabschiedet. Sie besteht aus zwei Teilen: Der erste Teil leitet aus den datenschutzrechtlichen Regelungen und den Vorgaben der ärztlichen Schweigepflicht konkrete rechtliche Forderungen für den Krankenhausbetrieb und die Anwendung von Informationssystemen in Krankenhäusern ab. Die Eckpunkte berücksichtigen bestehende Defizite und aktuelle Entwicklungen im Krankenhausbereich außerhalb der Forschung und formulieren auch Zielvorgaben, die in den vorhandenen Systemen derzeit noch nicht oder nur unzureichend abgebildet werden. Der zweite Teil beschreibt Maßnahmen zur technischen Umsetzung dieser Vorgaben wie auch allgemeingültiger datenschutzrechtlicher Regelungen, die für einen datenschutzgerechten Betrieb von Krankenhausinformationssystemen durch die Betreiber zu ergreifen sind, und stellt darüber hinaus Anforderungen an die Gestaltung von Softwareprodukten, die für die Verwendung innerhalb von Krankenhausinformationssystemen vorgesehen sind. Adressaten der Orientierungshilfe sind neben den anwendenden Krankenhäusern die Systemhersteller von Verarbeitungsprogrammen für Patientendaten.

Im August des Berichtsjahres informierten wir die Krankenhäuser im Land Bremen, die Dachgesellschaft der kommunalen Kliniken in Bremen und die Senatorin für Gesundheit über die Orientierungshilfe, um sicherzustellen, dass die datenschutzrechtlichen Anforderungen in den Kliniken im Land Bremen eingehalten werden.

7.2 „Kostenlose“ Babyfotos im Krankenhaus

Im November 2010 meldete sich ein Bürger, der über die Praxis im städtischen Klinikum Links der Weser berichtete, dass auf der Wochenstation Mütter von Neugeborenen durch einen externen Fotoservice aufgesucht würden, um die Neugeborenen zu fotografieren. Von dem Fotoservice wird für eine Glückwunschkarte der Klinik ein kostenloses Foto des Kindes zur Verfügung gestellt, das mit Einwilligung der Betroffenen auch in der Babygalerie auf der Klinikhomepage veröffentlicht wird. Weitere Fotos bietet der Fotoservice den Eltern kostenpflichtig an. Zu diesem Zweck sucht die Fotografin des Fotoservices regelmäßig die Wochenstation der Bremer Kliniken auf und erhält dort die Information über die neuen Geburten und die Zimmernummern der Mütter mit Neugeborenen. Sie sucht die Mütter dann in ihren Zimmern auf, um ihnen die Angebote des Fotoservices zu unterbreiten. Eine vorherige Information oder Einwilligung der betroffenen Mütter erfolgte nicht, was bei den betroffenen Müttern zum Teil auch einen Überrumpelungseffekt auslöste.

Von unserer Seite wurde darauf hingewiesen, dass es sich bei der Information der Fotografin über die Geburten der Wöchnerinnen durch die Mitarbeiterinnen und Mitarbeiter der Wochenstation um eine Übermittlung von Patientendaten an eine Stelle außerhalb des Krankenhauses handelt, die nur mit Einwilligung der Betroffenen zulässig ist. Von Seiten der Klinik wurde daraufhin ein Formular für eine entsprechende Einwilligungserklärung entwickelt und mit uns abgestimmt.

7.3 Akteneinsicht durch Abgeordnete

Das Amt für Soziale Dienste gewährte im Berichtsjahr zwei Abgeordneten der Bremischen Bürgerschaft, von denen eine Abgeordnete Mitglied der städtischen Deputation für Soziales, Jugend, Senioren und Ausländerintegration und ein Abgeordneter Mitglied des Rechtsausschusses und Rechnungsprüfungsausschusses war, Einsicht in die Akten eines Sozialhilfeempfängers. Im Anschluss an die Akteneinsicht in die 36 Bände umfassenden Sozialhilfeakten wurde von Seiten der Abgeord-

neten die Herausgabe einer kompletten Kopie der Akten gefordert. Dies wurde jedoch vom Sozialressort mit der Begründung abgelehnt, dass Kopien der Akten zu einem unverhältnismäßigen Aufwand und enormen Kosten führen würden, da personenbezogene Daten von Dritten in den Akten geschwärzt werden müssten. Es bestehe jedoch weiterhin die Möglichkeit, die Akten einzusehen; einzelne Seiten könnten auch kopiert werden.

Auf Nachfrage benannte uns das Amt für Soziale Dienste als Rechtsgrundlage für die Übermittlung der Sozialdaten an die beiden Abgeordneten § 16 des Gesetzes über die Deputationen. Schutzwürdige Belange des Betroffenen würden der Datenübermittlung nicht entgegenstehen, da dieser in dieser Angelegenheit selbst bereits mit der Presse gesprochen habe. Später wurde vom Amt für Soziale Dienste dargelegt, dass vom Sozialressort § 67 c Absatz 3 Satz 1 Sozialgesetzbuch (SGB) X als Rechtsgrundlage für die Übermittlung der Sozialdaten zum Zweck der Rechnungsprüfung angenommen worden sei.

Wir wiesen das Amt für Soziale Dienste darauf hin, dass eine Übermittlung von Sozialdaten nur zulässig ist, wenn eine Rechtsgrundlage im Sozialgesetzbuch dies erlaubt. Eine Rechtsgrundlage aus dem Sozialgesetzbuch, die eine Übermittlung von Sozialdaten an Abgeordnete beziehungsweise Mitglieder von Deputationen oder Ausschüssen erlaubt, gibt es nicht. Insbesondere kann die Datenübermittlung nicht auf § 69 Absatz 5 in Verbindung mit § 67 c Absatz 3 Satz 1 SGB X gestützt werden, wonach die Übermittlung von Sozialdaten zulässig ist für die Erfüllung der gesetzlichen Aufgaben der Rechnungshöfe und der anderen Stellen, auf die § 67 c Absatz 3 Satz 1 Anwendung findet. § 67 c Absatz 3 Satz 1 SGB X ist zwar anwendbar auf Aufsichtstätigkeiten, Kontrolltätigkeiten, Disziplinartätigkeiten, Rechnungsprüfungstätigkeiten und Prüftätigkeiten. Diese Ermächtigung gilt für die Dienstaufsicht und Fachaufsicht durch die jeweils übergeordnete öffentliche Stelle. Dazu gehören die städtischen Deputationen und Ausschüsse der Bürgerschaft nicht. Auch § 16 des Gesetzes über die Deputationen kann nicht als Rechtsgrundlage für die oben geschilderte Übermittlung der Sozialdaten herangezogen werden. Das Sozialgesetzbuch als Bundesgesetz ist im Verhältnis zum Deputationengesetz des Landes höherrangiges Recht. Läge ein Widerspruch zwischen diesen beiden Gesetzen vor, wäre nach dem Grundsatz Bundesrecht bricht Landesrecht nach Artikel 31 Grundgesetz allein die bundesgesetzliche Regelung des Sozialgesetzbuchs anwendbar. Das Bremische Deputationengesetz ist hier als untergeordnetes Landesrecht also bundesgesetzkonform auszulegen. Aufgrund der eindeutigen Einschränkung der Zulässigkeit der Übermittlung von Sozialdaten im Sozialgesetzbuch, die nicht durch das Deputationengesetz wieder erweitert werden kann, muss man bei der Anwendung des Bremischen Deputationengesetzes also zu dem Ergebnis kommen, dass die Erteilung von Auskünften oder die Vorlage von Akten abgelehnt werden muss, da hier überwiegende schutzwürdige Belange des Betroffenen entgegenstehen. Eine Bekanntmachung von Informationen aus seiner Sozialhilfeakte durch den Betroffenen selbst bei Gelegenheit eines Gespräches mit der Presse kann das Vorliegen einer gesetzlichen Rechtsgrundlage für die Übermittlung der Sozialdaten nicht ersetzen und ist daher unerheblich. Zudem geht die Gewährung von Akteneinsicht in die insgesamt 36 Aktenordner der Sozialhilfeakte des Betroffenen weit über die Weitergabe der Informationen des Betroffenen an die Presse hinaus. Daher war die Übermittlung der Sozialdaten an die beiden Abgeordneten unzulässig.

Das Amt für Soziale Dienste bestätigte schließlich, unsere Rechtsauffassung für die Zukunft zu übernehmen, solange keine anderslautende Weisung vom Sozialressort vorliegt.

Der dem Rechtsausschuss und dem Rechnungsprüfungsausschuss angehörende Abgeordnete der Bremischen Bürgerschaft stellte zusätzlich einen Antrag auf Akteneinsicht in die in diesem Fall vorhandenen staatsanwaltschaftlichen Strafakten und Ermittlungsakten. Ein entsprechender Beschluss wurde durch den Rechtsausschuss der Bremischen Bürgerschaft erlassen, ungeachtet dessen, dass es sich insoweit um ein laufendes Strafverfahren handelte. Dem Abgeordneten wurde daraufhin seitens des Senators für Justiz und Verfassung die begehrte Akteneinsicht gewährt. Vor der eigentlichen Einsichtnahme durch den Abgeordneten hatte dieser noch eine Erklärung unterschrieben, mit der er sich verpflichtete, über Informationen zu den persönlichen Verhältnissen des Betroffenen, insbesondere zu Namen und Anschriften, Gesundheitsdaten, Sozialdaten und Vorstrafen im Sinne von § 8 der Datenschutzordnung der Bremischen Bürgerschaft Verschwiegenheit zu bewahren.

Wir machten gegenüber dem Senator für Justiz und Verfassung unsere Rechtsauffassung deutlich, wonach das vorbeschriebene Vorgehen aus datenschutzrechtlicher Sicht problematisch ist, denn in den Strafverfahrensakten waren auch Sozialdaten des Betroffenen enthalten. Aus diesem Grunde hätten seitens des Senators für Justiz und Verfassung die datenschutzrechtlichen Bestimmungen im SGB X beachtet werden müssen. Danach ist eine Übermittlung von Sozialdaten nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den Vorschriften des SGB X dies erlaubt. Das ist indes nicht der Fall. Auch stellten wir gegenüber dem Senator für Justiz und Verfassung klar, dass kein Rückgriff auf die Vorschriften in der Strafprozessordnung möglich ist. Zwar gewährt die Strafprozessordnung grundsätzlich ein Akteneinsichtsrecht für am Strafverfahren Unbeteiligte. Allerdings muss dabei beachtet werden, dass dies nur dann gilt, wenn der Übermittlung keine besonderen bundesrechtlichen Verwendungsregelungen entgegenstehen. Genau das ist aber wegen der Vorschriften im SGB X der Fall.

Gegenstand des Meinungsaustausches mit dem Senator für Justiz und Verfassung war schließlich die Frage, inwieweit sich im zugrunde liegenden Fall etwas anderes aus der Bremischen Landesverfassung ergeben kann. Nach Artikel 105 Absatz 4 Satz 1 der Bremischen Landesverfassung können Ausschussmitglieder jederzeit die Einrichtungen des Aufgabenbereichs, für den der Ausschuss zuständig ist, besichtigen und in der Verwaltung dieses Bereichs Auskunft für die Ausschussarbeit einholen. Wir machten gegenüber dem Senator für Justiz und Verfassung deutlich, dass es uns nicht darum geht, die parlamentarischen Kontrollrechte der Abgeordneten zu beschränken oder gar zu verhindern. Bei der Gewährung von Akteneinsicht müssen jedoch nach der Regelung der Landesverfassung auch die schutzwürdigen Belange der Betroffenen berücksichtigt und in die Abwägung einbezogen werden. Damit trägt die landesverfassungsrechtliche Bestimmung dem Gewährleistungsgehalt der im Grundgesetz verankerten Grundrechte wie dem Recht auf informationelle Selbstbestimmung Rechnung. Zugleich spiegelt sich in der Norm der Grundsatz der Verhältnismäßigkeit wider. Wir vertraten deshalb die Auffassung, dass diesem Abwägungsprozess im vorliegenden Fall nicht hinreichend Rechnung getragen wurde. Zunächst stellt sich die Frage, ob die Einsichtnahme in die Strafakten des Betroffenen für die Erreichung des Ziels der parlamentarischen Kontrolle erforderlich waren, ging es doch aus Sicht des Antragstellers um die Kontrolle der Tätigkeit des Sozialressorts. Hinzu kam, dass sich das Akteneinsichtsgesuch auf einen Vorgang bezog, der noch nicht abgeschlossen war. Mit Rücksicht auf den Betroffenen hätte hier der Abschluss des Verfahrens abgewartet werden müssen. Wir wiesen den Senator für Justiz und Verfassung deshalb darauf hin, dass beim Abwägungsprozess in solchen Fällen eindeutig zum Ausdruck kommen muss, dass in die Abwägung auch die schutzwürdigen Belange des Betroffenen einbezogen worden sind. Das bloße Unterzeichnen einer Verschwiegenheitserklärung kann einen solchen Abwägungsprozess nicht ersetzen.

Wir erwarten, dass bei künftigen Akteneinsichtsanträgen durch Abgeordnete die möglicherweise entgegenstehenden überwiegenden schutzwürdigen Belange der beziehungsweise des Betroffenen berücksichtigt werden und dies dokumentiert wird und dass dabei berücksichtigt wird, dass Sozialdaten dem besonderen Schutz der Sozialgesetzbücher unterliegen.

7.4 Vorgaben für die Verarbeitung von Sozialdaten durch Träger der freien Jugendhilfe

Im Juli des Berichtsjahres wandten wir uns an das Amt für Soziale Dienste und teilten mit, dass sich in letzter Zeit vermehrt Mitarbeiterinnen und Mitarbeiter von freien Trägern der Jugendhilfe an uns gewandt und von erheblichen Defiziten bei der Einhaltung der Bestimmungen zum Sozialdatenschutz in ihren Einrichtungen berichtet haben. Berichtet wurde unter anderem von ungeschützter Verarbeitung von hochsensiblen Sozialdaten am Privatcomputer der Mitarbeiterinnen und Mitarbeiter, von offen zugänglicher Aufbewahrung und offenem Transport von Akten mit Sozialdaten, festen Löschfristen von zehn Jahren für nicht mehr benötigte Sozialdaten, unsachgemäßer Entsorgung von Sozialdaten und so weiter. Zum Teil würden sogar Sachbearbeiterinnen und Sachbearbeiter des Amtes für Soziale Dienste die Mitarbeiterinnen beziehungsweise die Mitarbeiter der freien Träger zur Versendung von Sozialdaten per E-Mail auffordern, ohne dass dafür eine geschützte Verbindung bereitgestellt würde. Die Hinweisgebenden berichteten zum Teil von einem Druck im Arbeitsverhältnis, sich an diesen von ihnen als unzumutbar emp-

fundenen Praktiken zu beteiligen. Hinweise auf die Unzulässigkeit würden oftmals nur als Störfaktor behandelt und hätten den Betroffenen zum Teil auch Nachteile bereitet. Andererseits würde auch von der Leitungsebene angeführt, dass es immer schwieriger würde, gegenüber den eigenen Mitarbeiterinnen und Mitarbeitern Vorgaben zum Datenschutz durchzusetzen, da diese bei anderen Trägern zum Teil nicht existierten.

Im Bereich der Jugendhilfe werden viele Aufgaben durch oder in Zusammenarbeit mit freien Trägern der Jugendhilfe erbracht. Die freien Träger sind keine Sozialleistungsträger im Sinne des Sozialgesetzbuches I. Für sie gelten die Regelungen zum Sozialdatenschutz im Sozialgesetzbuch daher nicht unmittelbar. Um einen den Regelungen des Sozialgesetzbuchs entsprechenden Schutz der Sozialdaten bei der Einschaltung durch freie Träger der Jugendhilfe zu schaffen, ist nach dem Sozialgesetzbuch VIII, soweit Einrichtungen und Dienste der Träger der freien Jugendhilfe in Anspruch genommen werden, sicherzustellen, dass der Schutz der personenbezogenen Daten bei der Erhebung und Verwendung in entsprechender Weise gewährleistet ist. Demnach ist der Träger der öffentlichen Jugendhilfe Garant dafür, dass der Datenschutz bei den freien Trägern adäquat beachtet wird.

Um sich der Beachtung des Datenschutzes durch die Träger der freien Jugendhilfe zu vergewissern, bedarf es einer konkretisierenden Auflistung der Interventionsbereiche und Interventionsmethoden sowie der praktischen Datenschutzvorkehrungen durch den Träger der öffentlichen Jugendhilfe. Um den gesetzlichen Anforderungen gerecht zu werden, sollte das Amt für Soziale Dienste den beauftragten freien Trägern insbesondere Vorgaben machen zur Verarbeitung von Sozialdaten in den folgenden Bereichen:

— Verschwiegenheitsverpflichtungen,

— Umfang der zulässigen Datenerhebung,

— sachgemäße Aufbewahrung und Entsorgung von Papierakten,

— Datenübermittlungsbefugnisse,

— Löschverpflichtungen,

— elektronische Datenverarbeitung innerhalb und außerhalb der Geschäftsräume der freien Träger (technische und organisatorischen Maßnahmen),

— Betroffenenrechte: Auskunft/Akteneinsicht, Berichtigung, Löschung, Sperrung, Widerspruchsrecht,

— eventuell erforderliche datenschutzrechtliche Einwilligungserklärungen.

Wir baten das Amt für Soziale Dienste um Mitteilung, welche Vorgaben, Empfehlungen, Richtlinien oder ähnliches es den bei der Aufgabenerfüllung im Bereich der Jugendhilfe eingesetzten freien Trägern vorgibt beziehungsweise zur Verfügung stellt und wie die Einhaltung dieser Vorgaben überprüft wird.

Anfang September 2011 teilte uns das Amt für Soziale Dienste mit, dass es leider noch nicht gelungen sei, flächendeckend sichere Übertragungswege für eine elektronische Kommunikation einzurichten. Daran werde jedoch gearbeitet. In Bezug auf die Vorgaben für die freien Träger werde unsere Auffassung zur Notwendigkeit der Vorgaben geteilt, jedoch besitze das Amt für Soziale Dienste spätestens nach der letzten organisatorischen Änderung im Bereich des Ressorts Soziales, Kinder, Jugend und Frauen, der Zusammenlegung der Fachabteilungen in der senatorischen Behörde, nicht mehr die Kompetenz, entsprechende Rahmenvereinbarungen beziehungsweise Vorgaben mit freien Trägern der Jugendhilfe zu treffen. Insoweit wurden wir auf die Zuständigkeit der Senatorin für Soziales, Kinder, Jugend und Frauen verwiesen.

Daraufhin richteten wir unsere Anfrage an die senatorische Behörde, die daraufhin Handlungsbedarf in dieser Hinsicht bestätigte.

Wir wurden dann von der senatorischen Behörde um datenschutzrechtliche Prüfung eines Folge-Kooperationsvertrages des Amtes für Soziale Dienste und der senatorischen Behörde mit einem freien Träger, dem öffentliche Aufgaben im Bereich Vollzeitpflege, Kurzzeitpflege, Kindertagespflege, Patenschaften und Übergangspflegestellen übertragen worden sind, gebeten. In diesem Zusammenhang verwiesen wir auf die oben ausgeführte Notwendigkeit der Vorgaben zum Datenschutz von Seiten des Trägers der öffentlichen Jugendhilfe. Die Ausführungen zum Da-

tenschutz im Ende 2011 auslaufenden Kooperationsvertrag genügten diesen Anforderungen nicht. Wir unterstützten das Amt und die beiden Behörden daher bei der Erarbeitung von datenschutzrechtlichen Vorgaben aufgrund einer Risikoanalyse anhand der speziellen Verhältnisse beim Träger, die in den Vertrag mit aufgenommen wurden. Insbesondere wurden für den Umgang mit personenbezogenen Daten der Klientinnen beziehungsweise Klienten beim Träger die Regelungen des Sozialgesetzbuchs VIII und X für anwendbar erklärt. Konkret wurden die Befugnisse zur Datenerhebung, Datenübermittlung und Datennutzung erläutert und es wurde auf die Verpflichtung zur Erfüllung des datenschutzrechtlichen Auskunftsanspruchs und die Erarbeitung eines Löschkonzeptes hingewiesen. Des Weiteren wurden Vorgaben zur Abgabe einer Verschwiegenheitsverpflichtung der Mitarbeiterinnen und Mitarbeiter, zur Bestellung einer beziehungsweise eines behördlichen Datenschutzbeauftragten sowie zur Erstellung eines Datenschutzkonzeptes für automatisierte Verfahren gemacht. Der Transport von Akten mit personenbezogenen Daten außerhalb der Geschäftsräume wurde ebenso untersagt wie der Einsatz von mobilen elektronischen Endgeräten und privaten Computern und die unverschlüsselte Versendung von personenbezogenen Daten.

7.5 Konzept zur Umsetzung eines präventiven Kinderschutzes

Im August des Berichtsjahres erfuhren wir vom Senator für Inneres und Sport von dem Projekt Hausbesuche „Willkommen an Bord“ des Konzepts zur Umsetzung eines präventiven Kinderschutzes im Amt für Jugend, Familie und Frauen als Jugendamt der Stadt Bremerhaven. Im entsprechenden Rahmenkonzept wird ausgeführt, dass damit ein systematisch abgestimmtes Verfahren zur rechtzeitigen Einschätzung von Gefährdungslagen, ein soziales Frühwarnsystem zur Wahrnehmung riskanter Lebenssituationen bei Kindern und deren Familien aufgebaut wird, um frühzeitig handeln zu können. Zu diesem Zweck erhalten alle Familien mit einem Neugeborenen in Bremerhaven, alle Familien mit Kindern unter 6 Jahren, die nach Bremerhaven ziehen, und alle Familien mit Kindern, die mit 3 Jahren nicht in der Kindertagesstätte angemeldet werden, einen Hausbesuch. Bei diesem Hausbesuch werden Glückwünsche und ein Präsent des Magistrats der Stadt Bremerhaven und Informationsmaterial überbracht. Zudem wird vor Ort Hilfe in Angelegenheiten wie zum Beispiel dem Antrag auf Kindergeld, Elterngeld, Hebammenleistungen, Vergünstigungen und so weiter angeboten. Die Eltern werden über familienrelevante Dienstleistungen und Hilfen der Stadt Bremerhaven informiert und bei Bedarf werden unverzüglich niederschwellige Hilfen installiert. Wenn bei dem Hausbesuch Anhaltspunkte für eine Nichtgewährleistung oder gar Gefährdung des Kindeswohls festgestellt werden, teilen die Mitarbeiterinnen und Mitarbeiter des Besuchsdienstes den Eltern mit, dass sie den Ambulanten Sozialdienst informieren, damit dieser sofort im Rahmen des Verfahrens „Kindeswohlsicherung“ tätig wird. Zu diesem Zweck soll ein automatisiertes Abrufverfahren für das Jugendamt auf die Daten des Melderegisters eingerichtet werden. Das Jugendamt soll die Daten der identifizierten Risikofamilien im Melderegister abrufen und an die Arbeiterwohlfahrt Sozialdienste GmbH übermitteln. Die Arbeiterwohlfahrt Sozialdienste GmbH nutzt die übermittelten Daten, um die Begrüßungsschreiben zu versenden, die Hausbesuche durchzuführen, die eventuell erforderlichen Beratungen vor Ort durchzuführen und zu prüfen, ob Anhaltspunkte für eine Kindeswohlgefährdung bestehen.

In einer Vereinbarung des Amtes für Jugend, Familie und Frauen der Stadt Bremerhaven als Auftraggeber und der Arbeiterwohlfahrt Sozialdienste GmbH Bremerhaven als Auftragnehmerin wird die Übertragung der Aufgaben der Adressierung und Versendung des Begrüßungsschreibens der Stadt Bremerhaven, der Durchführung der Hausbesuche sowie der Führung einer quantitativen nicht personenbezogenen Statistik auf die Arbeiterwohlfahrt Sozialdienste GmbH geregelt. Die Formulierung der Vereinbarung lässt darauf schließen, dass die Beteiligten dabei von einer Auftragsdatenverarbeitung ausgegangen sind. So wird eine Verantwortlichkeit des Auftraggebers für die Zulässigkeit der Datenverarbeitung und die Wahrung der Betroffenenrechte sowie Kontrollrechte durch Akteneinsicht festgelegt.

Wir teilten dem Amt für Jugend, Familie und Frauen mit, dass die Übermittlung der Adressdaten der hier ausgewählten Personenkreise vom Meldeamt an das Jugendamt nicht zulässig ist, da es keine Rechtsgrundlage gibt, die dem Jugendamt die Erhebung von Adressdaten zum Zweck der Durchführung von Hausbesuchen erlaubt. Auch § 16 des Sozialgesetzbuches VIII kommt als Aufgabenzuweisungs-

norm hier nicht in Betracht, da diese Regelung keinen Umgang mit personenbezogenen Daten vorsieht. Wir wiesen auf das sogenannte Adressmittlungsverfahren als datenschutzkonforme Lösungsmöglichkeit hin, bei dem das Jugendamt den Meldebehörden vorbereitete Schreiben an die Betroffenen zur Verfügung stellt, die dann von den Meldebehörden unter Nutzung der bei ihnen vorhandenen Daten versandt werden können. Bei dieser Variante könnten sich die Eltern, die das Angebot eines Hausbesuchs wahrnehmen möchten, an das Jugendamt wenden. Ein anlassloser Hausbesuch durch Mitarbeiterinnen und Mitarbeiter des Jugendamtes wäre nur dann datenschutzrechtlich zulässig, wenn die Eltern freiwillig und informiert – das heißt insbesondere in Kenntnis der beabsichtigten Datenerhebung des Jugendamtes beim Hausbesuch – einen solchen Hausbesuch ausdrücklich wünschen oder ihre Einwilligung dazu gegenüber dem Jugendamt erklären. Dies setzt voraus, dass die Betroffenen über die Freiwilligkeit der Besuche, die Identität der verantwortlichen Stelle und über die verfolgten Zwecke hinreichend aufgeklärt wurden. Datenschutzrechtlich höchst bedenklich wäre es, anlässlich eines Hausbesuchs zum Zweck der allgemeinen Familienförderung eine heimliche, beziehungsweise über den angegebenen Zweck hinausgehende Datenerhebung ohne vorherige Aufklärung der Eltern durchzuführen.

Hinzu kommt, dass die Beauftragung der Arbeiterwohlfahrt Sozialdienste GmbH nicht als Verarbeitung von Sozialdaten im Auftrag nach dem Sozialgesetzbuch X ausgestaltet werden kann, da Gegenstand des Auftrages nicht die Erhebung, Nutzung oder Verarbeitung von Sozialdaten, also das Speichern, Verändern, Übermitteln, Sperren oder Löschen von Sozialdaten, sondern die gesamte Aufgabe der Durchführung der Hausbesuche einschließlich Beratung und gegebenenfalls Vermittlung von weiteren Hilfen übertragen werden soll. Eine Datenübermittlung von der Arbeiterwohlfahrt Sozialdienste GmbH an das Jugendamt in Bezug auf Anhaltspunkte für Kindeswohlgefährdungen darf nach dem Sozialgesetzbuch VIII nur erfolgen, wenn die Fachkräfte des freien Trägers das Gefährdungsrisiko im Zusammenwirken mit einer erfahrenen Fachkraft selbst abgeschätzt und bei den Personensorgeberechtigten oder den Erziehungsberechtigten auf die Inanspruchnahme von den für erforderlich gehaltenen Hilfen hingewirkt haben und die angenommenen Hilfen nicht ausreichend erscheinen, um die Gefährdung abzuwenden.

Die Möglichkeit des Einsatzes eines Adressmittlungsverfahrens wurde vom Amt für Jugend, Familie und Frauen abgelehnt mit der Begründung, dass auf diese Weise nicht genügend Familien erreicht werden könnten. Von dort wurde signalisiert, dass man sich um die Schaffung einer gesetzlichen Rechtsgrundlage für die Erhebung von Meldedaten zum Zweck der Durchführung von Hausbesuchen bemühen werde.

Da die aktuelle Rechtslage eine entsprechende Datenerhebung nicht erlaubt, muss diese zunächst eingestellt werden.

7.6 Anforderung von medizinischen Unterlagen bei Pflegediensten

Ein ambulanter Pflegedienst wandte sich an uns und berichtete, dass von einer Bremer Krankenkasse regelmäßig mit der Mitteilung über die Kostenübernahme für die häusliche Krankenpflege medizinische Unterlagen der Patientinnen und Patienten (Blutzucker-Messprotokolle, Auflistung der verabreichten Bedarfsmedikation, Wundberichte mit Behandlungsplan, Bilder der Wunde) angefordert würden. Für eine nicht rechtzeitige beziehungsweise nicht vollständige Übersendung der angeforderten Unterlagen würde eine Kürzung der Kostenübernahme in Aussicht gestellt. Auf den Anforderungsschreiben würde zwar mitgeteilt, dass diese Unterlagen für den Medizinischen Dienst der Krankenversicherung (MDK) angefordert würden. Auf eine Übersendung der Unterlagen in einem verschlossenen Umschlag, auf dem vermerkt wird, dass dieser nur vom MDK geöffnet werden darf, werde jedoch nicht hingewiesen. Häufig würden die Unterlagen auch lediglich telefonisch angefordert.

Eine Anforderung von medizinischen Unterlagen durch die Krankenkasse ist für deren Aufgabenerfüllung nach § 37 Sozialgesetzbuch V nicht erforderlich und daher auch nicht zulässig. Bei Zweifeln der Krankenkasse über ihre Verpflichtung zur Leistung ist nach diesem Gesetz der MDK einzuschalten. Gegen die Anforderung von Unterlagen für den MDK, die bei der Krankenkasse nicht eingesehen werden, bestehen aus datenschutzrechtlicher Sicht keine Bedenken.

Auf Nachfrage teilte die Krankenkasse mit, dass sie nach den Richtlinien zur häuslichen Krankenpflege verpflichtet sei, bei der Prüfung der Kostenübernahme bei

Verordnungen zur häuslichen Krankenpflege neben den versicherungsrechtlichen auch die leistungsrechtlichen Voraussetzungen zu prüfen. Zu diesem Zweck seien die Angaben auf den eingereichten Verordnungen aber oftmals nicht detailliert genug, sodass eine Beurteilung nach Aktenlage nicht möglich sei. Daher werde der Medizinische Dienst der Krankenversicherung zur Unterstützung herangezogen. Nach den Richtlinien zur Zusammenarbeit der Krankenkassen mit dem MDK habe die Krankenkasse sich davon zu überzeugen, dass die Angaben in der ärztlichen Verordnung vollständig und plausibel seien und eventuell fehlende Angaben, Unklarheiten oder Unstimmigkeiten mit der behandelnden Ärztin beziehungsweise dem behandelnden Arzt oder sonstigen Leistungserbringern zu ergänzen oder zu klären. Es sei Aufgabe der Krankenkasse, dem MDK prüffähige Unterlagen vorzulegen. In der Praxis würden daher in diesen Fällen für den MDK Unterlagen entweder bei der behandelnden Ärztin beziehungsweise beim behandelnden Arzt oder bei den Pflegediensten angefordert. Diese würden von der Krankenkasse jedoch nicht eingesehen, gespeichert, genutzt oder bewertet. Bisher sei in den Anforderungsschreiben nicht darauf hingewiesen worden, dass die Unterlagen in einem verschlossenen Umschlag zugeschickt werden sollten. Dies werde jedoch zukünftig erfolgen.

Wir begrüßten es, dass die Unterlagen für den MDK zukünftig unter Hinweis auf die Verwendung eines an den MDK adressierten verschlossenen Umschlags angefordert werden sollen. Diesbezüglich baten wir darum, die erforderlichen Maßnahmen zu treffen um sicherzustellen, dass dieser Hinweis gegenüber den Pflegediensten oder behandelnden Ärzten auch bei telefonischen Anforderungen erteilt wird und dass die eingehenden Umschläge durchgängig ungeöffnet an den MDK weitergeleitet werden.

7.7 Bericht aus dem Arbeitskreis Gesundheit und Soziales

Im Arbeitskreis Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurden im Berichtsjahr unter anderem die folgenden Themen behandelt: elektronischer Entgeltnachweis (ELENA), Einrichtung eines „Runden Tisches Heimerziehung in den 50er und 60er Jahren“ durch den Petitionsausschuss des Deutschen Bundestages, Erhebung der Steuer-Identitätsnummer durch die gesetzlichen Krankenkassen beim Bundeszentralamt für Steuern, Ambulante Kodierrichtlinien, Forschungsvorhaben von Kassenärztlichen Vereinigungen und dem Zentralinstitut für die kassenärztliche Versorgung in Deutschland und Kontrolle der Datenverarbeitung beim Zentralinstitut für die kassenärztliche Vereinigung, Internetrecherche durch Jugendämter, Regelung von „Selektiv-Verträgen“, insbesondere von hausarztzentrierten Versorgungsverträgen, Verwendung des E-Postbriefs der Deutschen Post in der Sozialverwaltung, Datenerhebungen durch Krankenkassen/Pflegekassen bei Versicherten, Ärztinnen und Ärzten und Pflegediensten, Krankenhausinformationssysteme, Elektronische Gesundheitskarte, Nationales Krebsregister, Mammographie-Screening, Begrüßungsbesuche bei Neugeborenen, Durchführung von Prüfungen zur Qualitätssicherung durch ärztliche Stellen nach § 17 a Röntgenverordnung, Pflegestützpunkte, Regelungen zu Leistungen für Bildung und Teilhabe („Bildungspaket“), Kompetenzzentren bei Kassenärztlichen Vereinigungen, Patientenidentifikation im Krankenhaus mittels Patientenarmbändern, Nutzung von De-Mail durch gesetzliche Krankenkassen und andere Sozialleistungsträger, Einbindung von gesetzlichen Krankenkassen im Rahmen sozialer Netzwerke, Telearbeit mit Sozialdaten und Projekt „Nationale Kohorte“.

8. Bildung, Wissenschaft und Kultur

8.1 Beratungsgeheimnis bei der Raumplanung für regionale Beratungszentren

Ein Beratungszentrum war in ein Schulgebäude umgezogen. Wir erfuhren von Befürchtungen, das Beratungsgeheimnis würde in den bezogenen ehemaligen Klassenräumen nicht eingehalten werden können. Den Angaben zufolge sollten nur zwei Beratungsräume vorgehalten werden. In den restlichen zwei bis drei Räumen sollten insgesamt neun Schulpsychologinnen und Schulpsychologen, Sozialarbeiterinnen und Sozialarbeiter und andere Beschäftigte arbeiten. Mehr Räume seien nicht vorhanden. Die Tätigkeit dieses Personenkreises betreffe vorwiegend Diagnostik und Beratung, sodass ihre Tätigkeit der Schweigepflicht und dem besonderen Beratungsgeheimnis unterliege. Würden sich diese Beschäftigten zu zweit oder dritt ein Zimmer teilen, würde diese räumliche Situation beim Führen von Telefon-

gesprächen oder im Fall spontaner Besuche von Petentinnen und Petenten das Beratungsgeheimnis gefährden.

In einem Gespräch mit der Bildungsbehörde zur Frage, welche technischen und organisatorischen Maßnahmen zur Einhaltung des Beratungsgeheimnisses getroffen werden können, wurde Folgendes vereinbart:

Wenn wegen großer Klassenräume mit durchgehender Fensterfront eine Raumteilung nicht möglich ist und nicht für alle Beraterinnen und Berater ein Einzelzimmer zur Verfügung gestellt werden kann, sollen ausreichende Besprechungsräume beziehungsweise Beratungsräume hergerichtet werden. Außerdem soll festgelegt werden, wie bei vertraulichen Telefongesprächen mit Klientinnen und Klienten umzugehen ist, wenn eine Kollegin oder ein Kollege im gleichen Zimmer arbeitet und den Raum wegen der eigenen Arbeit nicht vorübergehend verlassen kann.

Das Bildungsressort hat die Problematik erkannt und zugesagt, angemessene Vorkehrungen zur Einhaltung des Beratungsgeheimnisses zu schaffen.

8.2 „Stopp der Jugendgewalt“ – Einrichtung von Interventionsteams

Die Senatorin für Bildung, Wissenschaft und Gesundheit legte uns den Entwurf einer Kooperationsvereinbarung zwischen ihrem Ressort, der Polizei Bremen und dem Amt für Soziale Dienste zur Stellungnahme vor. Hierbei geht es um die sozialräumliche Zusammenarbeit in ressortübergreifenden Interventionsteams im Rahmen des Konzepts „Stopp der Jugendgewalt“.

Auftrag und Zielsetzung der Interventionsteams ist danach eine fallübergreifende Situationsanalyse und Situationsbewertung als Reaktion auf herausragende Problemkonstellationen durch Gewalt. Es wird für den umfangreichen Austausch personenbezogener Daten zwischen den Beteiligten des jeweiligen Interventionsteams (Beschäftigte von Polizei, Jugendamt, regionales Beratungszentrum und weitere Dritte) darauf verwiesen, dass dieser in Kenntnis und mit Zustimmung der Betroffenen erfolgen soll. Aus dem Entwurf war nicht zweifelsfrei erkennbar, welche personenbezogenen Daten anlässlich eines konkreten Vorfalls ausgetauscht werden sollen und ob im Vorfeld der Zusammenkunft eines Interventionsteams eine schriftliche Einwilligung beziehungsweise eine Schweigepflichtentbindungserklärung der oder des Betroffenen eingeholt werden sollen.

Inzwischen hat das Ressort den Entwurf überarbeitet. Er enthält nunmehr als Anlage alle wesentlichen besonderen Rechtsvorschriften. Allerdings werden diese Rechtsvorschriften für die Jugendhilfe, Polizei und Schule im Entwurf nicht hinreichend erläutert, sodass wir hierzu ergänzende Vorschläge unterbreitet haben. Ziel muss sein, den Beteiligten der Interventionsteams deutlich zu machen, unter welchen Voraussetzungen welche personenbezogenen Daten erhoben, gespeichert, übermittelt und genutzt werden dürfen. Es sollte auf konkrete Formulierungen geachtet werden, um Missverständnisse zu vermeiden.

Zudem ist konkret festzulegen, in welcher Weise die oder der Betroffene über einen zulässigen, auf einer entsprechenden Rechtsgrundlage beruhenden Datenaustausch in Kenntnis gesetzt wird.

Bezüglich der Wirksamkeit von Einwilligungen in „Fallkonferenzen“, in denen ein Austausch von mehr als zwei Stellen stattfindet, halten wir an unserer schon in den beiden Vorjahresberichten vertretenen Rechtsaufassung fest (siehe 32. Jahresbericht, Ziffer 5.2 und 33. Jahresbericht, Ziffer 5.8). Danach ist die Einholung von Einwilligungen in den Fällen unzulässig, in denen gesetzliche Datenübermittlungsbefugnisse aufgrund bewusster Entscheidung des Gesetzgebers fehlen. Wir nahmen gleichwohl zum vom Ressort übersandten Entwurf einer Einwilligungserklärung Stellung und wiesen unter anderem darauf hin, dass bei der Einholung sicherzustellen ist, dass keinerlei Druck auf Betroffene beziehungsweise deren Personensorgeberechtigte ausgeübt wird. Dem oder der Betroffenen müssen durch Aufklärung die Tragweite ihrer oder seiner Entscheidung und somit die Konsequenzen einer erteilten Einwilligung oder Verweigerung deutlich werden. Außerdem müssen im Text über die konkreten Ziele des Einsatzes eines Interventionsteams sowie über Art, Umfang, Zweck der Datenverarbeitung und bei einer Übermittlung zusätzlich die Empfänger der Daten benannt werden. Des Weiteren muss über die Folgen des Widerrufs und der Verweigerung der Einwilligung informiert werden.

Soweit auch in die Verarbeitung von Gesundheitsdaten, die ethnische Herkunft oder andere besondere Arten von Daten eingewilligt werden soll, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

8.3 Konzept Bildung und Teilhabe und „Blaue Karte“

Zur Umsetzung des Programms Bildung und Teilhabe legte die Senatorin für Bildung, Wissenschaft und Gesundheit ein Konzept vor. Danach erhalten alle Betroffenen vom Amt für Soziale Dienste eine sogenannte Blaue Karte, mit der sie den Nachweis erbringen, antragsberechtigt zu sein. Die Kosten für die Leistungen sollen die Schulen und Schulverwaltungen listenmäßig mit den Sozialleistungsträgern abrechnen. Zur Erhebung und Speicherung der dazu erforderlichen Daten soll die Verordnung über die Datenverarbeitung durch Schulen und Schulbehörden ergänzt werden.

Wir wiesen das Bildungsressort darauf hin, dass die Verordnungsermächtigung nur erlaubt die Speicherung von Daten zu regeln, nicht jedoch deren Übermittlung. Soweit personenbezogene Daten von Schülerinnen und Schüler an Sozialleistungsträger zur Abrechnung der Leistungen übermittelt werden sollen, bedarf es einer entsprechenden gesetzlichen Regelung. Eine solche befindet sich jedoch weder im Bremischen Schuldatenschutzgesetz noch in einem anderen Gesetz. Hier handelt es sich um eine Datenübermittlung für die Durchführung des neuen Bildungspakets und Teilhabepakets und um die Übermittlung von Sozialdaten. Aus diesem Grund halten wir es für unabdingbar, eine entsprechende spezielle Übermittlungsvorschrift im Bremischen Schuldatenschutzgesetz zu schaffen.

Außerdem haben wir vorgeschlagen, den Entwurf der Verordnung über die Datenverarbeitung durch Schulen und Schulbehörden dahingehend zu ergänzen, dass diese Daten unmittelbar nach Beendigung der Leistungen für Bildung und Teilhabe gelöscht werden.

Da die Daten im elektronischen Schulverwaltungssystem gespeichert werden sollen, haben wir zudem angeregt zu prüfen, ob das elektronische Schulverwaltungssystem für die Speicherung von Sozialdaten mit hohem Schutzbedarf überhaupt geeignet ist. Des Weiteren halten wir es für unabdingbar, diese Daten unverzüglich nach Beendigung der Geltungsdauer des Bezugs von Sozialleistungen zu löschen. Dazu baten wir das Ressort darzulegen, welche technischen Maßnahmen eine automatische Löschung der Daten gewährleisten sollen.

Zum Bildungspaket und Teilhabepaket liegen bei uns bereits einzelne Eingaben vor. Danach erklärten beispielsweise Eltern, die Schule ihres Kindes habe erklärt, die Blaue Karte müsse der Klassenlehrerin oder dem Klassenlehrer vorgelegt werden. Sie oder er benötige die Informationen für die Organisation von Klassenfahrten und Ausflügen oder für einen eventuellen Bedarf an Nachhilfe. Die betroffenen Eltern sind jedoch sogenannte Aufstocker, die nicht wollen, dass die Klassenlehrerin oder der Klassenlehrer davon Kenntnis erhält.

Aus diesem Grund regten wir beim Bildungsressort an, in dem vorgelegten Musterschreiben an die Erziehungsberechtigten für Klassenfahrten und Schulausflüge vorzusehen, dass die Blaue Karte nicht der Schule, sondern explizit dem Schulsekretariat vorgelegt werden muss.

Dies hat das Ressort zugesichert. Allerdings erhalte die Klassenlehrerin oder der Klassenlehrer indirekt Kenntnis über den Bezug von Sozialleistungen. Der Schulgesetzgeber erwarte von den Lehrkräften Kenntnis über die Lebensbedingungen der Schülerinnen und Schüler, ohne diese die Lehrkräfte ihren Erziehungsauftrag nicht erfüllen könnten. Es sei zudem lebensfremd, dass in einer Klassengemeinschaft die sozialen Bedingungen einzelner Schülerinnen und Schüler unbekannt blieben, beispielsweise durch Kleidung und Ausstattung von Schülerinnen und Schülern, Erzählungen über die häuslichen Bedingungen sowie die Berufe der Eltern.

Daraufhin legten wir dem Bildungsressort dar, dass die rechtlichen Anforderungen gleichwohl einzuhalten sind. Eine weitere Eingabe betraf die Farbe der Karte. Moniert wurde, hier könnten andere sich im Schulsekretariat aufhaltende Personen den Sachverhalt des Sozialleistungsempfangs erfahren. Eine weiße Karte sei insoweit neutraler. Dazu baten wir das Bildungsressort zu prüfen, inwieweit in den Schulsekretariaten die Vertraulichkeit der Antragstellung gewährleistet wird und ob nicht zukünftig eine weiße statt der blauen Karte verwendet werden kann.

8.4 Weiterleitung sensibler Schülerdaten innerhalb und außerhalb der Schule per E-Mail

Unsere Untersuchungen ergaben, dass in einer bremischen Privatschule teilweise sensible Schülerdaten wie Abiturgutachten, Noten sowie Gesundheitsgutachten innerhalb der Schule und der Lehrerschaft – auch an die Privatrechner der Lehrkräfte zu Hause – per unverschlüsselter E-Mail weitergeleitet wurden. Des Weiteren wurden häufig Dokumente mit diesen Schülerdaten über Verteiler der Schule unter Einschluss aller E-Mail-Adressen der Lehrkräfte der Schule auf diesem Wege weitergeleitet. Da der unverschlüsselte E-Mail-Verkehr keine vertrauliche Kommunikation darstellt, bedeutet dies, dass Unbefugte innerhalb und außerhalb der Schule Kenntnis über die Daten der Schülerinnen und Schüler erhalten und sie inhaltlich ändern könnten.

Die Privatschule erklärte dazu, sie verwende eine Verschlüsselung, die jedoch durch jede Nutzerin oder jeden Nutzer abgeschaltet werden könne. Insoweit kann jedoch nicht von einer durchgängigen angemessenen Transportverschlüsselung ausgegangen werden. Zur Frage der Verteilerliste legten wir dar, dass die Empfängerinnen und Empfänger der E-Mails diese ohne Weiteres von ihrem häuslichen Bereich an Dritte weiterleiten können. Der Hinweis, die Schulbehörde sei bisher nicht auf ihre Vorschläge zu einer hochwertigen Verschlüsselung eingegangen, befreit die Privatschule nicht von der Einhaltung angemessener Datensicherungsmaßnahmen.

Die Weiterleitung dienstlicher E-Mails mit sensiblen Schülerdaten an private E-Mail-Adressen ist nicht vertretbar. Die Weiterleitung passierte vermutlich unabhängig davon, ob die eingehende E-Mail von außerhalb oder von innerhalb der Domain gesendet wurden. Ebenso konnten Versenderinnen und Versender der Daten niemals sicher sein, ob diese an Dritte weitergeleitet wurden oder nicht. Die Privatschule hatte offensichtlich überhaupt keine Kontrolle darüber, welche Daten wo gespeichert und verarbeitet wurden. Es ist sehr wahrscheinlich, dass die Daten in das nicht europäische Ausland gelangen, beispielsweise wenn internationale Anbieter von E-Mail-Diensten genutzt werden. Dabei kann nicht von einem gleichen Datenschutzniveau wie innerhalb der Europäischen Union ausgegangen werden. E-Mails mit sensiblen Daten von Schülerinnen und Schülern dürfen daher niemals an derartige E-Mail-Adressen weitergeleitet werden. Da das alles technisch schwierig zu regeln ist, ist eine Weiterleitung von E-Mails mit sensiblen Daten von Schülerinnen und Schüler an private E-Mail-Adressen nicht zulässig.

Aus diesen Gründen haben wir die Privatschule aufgefordert, unverzüglich zu veranlassen, dass ab sofort personenbezogene Daten der Schülerinnen und Schüler weder innerhalb noch außerhalb der Schule per E-Mail versandt werden. Inzwischen hat die Schule mitgeteilt, eine Anweisung erlassen zu haben, dass die Weiterleitung dieser Daten per E-Mail nunmehr untersagt ist. Da nicht auszuschließen ist, dass auch Schulen in öffentlicher Trägerschaft E-Mails mit Daten der Schülerinnen und Schüler unverschlüsselt weiterleiten, baten wir die Senatorin für Bildung, Wissenschaft und Gesundheit, uns über das dortige Verfahren zu unterrichten.

9. Umwelt, Bau und Verkehr

9.1 Microsoft Bing Maps

Im letzten Tätigkeitsbericht betrachteten wir den Panoramadienst Google Street View aus datenschutzrechtlicher Sicht (siehe 33. Jahresbericht, Ziffer 1.1). Im aktuellen Berichtsjahr ist die datenschutzrechtliche Einordnung des Konkurrenzproduktes Bing Maps Streetside der Firma Microsoft berichtenswert. Seit Mai 2011 werden in einigen Regionen Deutschlands Kamerafahrten durchgeführt, die sich über circa 18 Monate erstrecken sollen. Wie auch die Firma Google im Falle ihrer Anwendung Street View, hatte Microsoft den Bürgerinnen und Bürgern die Möglichkeit eingeräumt, gegen die Veröffentlichung von Gebäudeansichten einen Vorabwiderspruch einzulegen. Auch hier geschah dies, ohne dass hierfür eine Rechtspflicht gesehen wurde, von der die datenschutzrechtlichen Aufsichtsbehörden aber weiterhin ausgehen. Microsoft hat angekündigt, Widersprüche, die nach dem 30. September 2011 eingegangen sind, nicht mehr vor der Veröffentlichung zu berücksichtigen. Auch zum jetzigen Zeitpunkt sei der Widerspruch möglich, jedoch werde eine Bearbeitung durch Microsoft erst erfolgen, nachdem der Internetdienst online gegangen ist.

9.2 Weitergabe von personenbezogenen Daten durch ein Taxiunternehmen

Im Berichtsjahr erreichte uns die Eingabe eines Bürgers, der sich bei einer Taxivermittlungszentrale sowie der Aufsichtsbehörde für das Taxigewerbe darüber beschwert hatte, dass ihm auf seine Anforderung hin zeitnah kein Taxi zur Verfügung gestellt werden konnte. Die Taxivermittlungszentrale hatte die Beschwerde, welche personenbezogenen Daten wie Name, Vorname, Anschrift, E-Mail-Adresse und Telefonnummer des Petenten enthielt, zur Verdeutlichung des Problems an die angeschlossenen Taxiunternehmen gesandt. Der Petent befürchtete, dass seine Daten dadurch einer großen Anzahl von Taxifahrerinnen und Taxifahrern zugänglich gemacht worden seien, da er seit dem Vorfall nachts anonyme Anrufe erhalte, die er mit der Datenübermittlung in Verbindung bringe.

Wir baten die Taxivermittlungszentrale um Stellungnahme und wiesen darauf hin, dass im vorliegenden Fall eine Übermittlung der Daten des Petenten nicht erforderlich gewesen war, um die Ernstlichkeit der Beschwerde zu verdeutlichen. Vor Weiterleitung der Beschwerde hätten die personenbezogenen Daten des Betroffenen unkenntlich gemacht werden müssen, da anderenfalls die Gefahr besteht, dass die Daten missbräuchlich verwendet werden. Das Beschwerdeschreiben des Bürgers an die Taxivermittlungszentrale kann auch nicht als stillschweigende Einverständniserklärung in eine Datenübermittlung gewertet werden. Das Bundesdatenschutzgesetz stellt an eine wirksame Einwilligung besondere Anforderungen, um dem Schutz von personenbezogenen Daten gerecht zu werden und keine leichtfertige Umgehung des Datenschutzes zu ermöglichen. Diese Voraussetzungen lagen im konkreten Fall nicht vor.

Wir wiesen das Unternehmen ausdrücklich auf die Rechtslage hin und forderten es auf, in Zukunft die geltenden datenschutzrechtlichen Vorschriften zu beachten.

9.3 Datenübermittlung zwischen Vermieter und Jobcenter

Ein Bürger wandte sich mit der Vermutung an uns, dass sein Vermieter personenbezogene Daten über ihn an das Jobcenter weitergegeben haben könnte. Ein uns vorliegendes Schreiben belegte, dass dem Jobcenter vom Vermieter mitgeteilt worden war, die vom Petenten angemietete Wohnung erwecke einen unbewohnten Eindruck. Für den Petenten war nicht nachvollziehbar, woher der Vermieter wusste, dass er Kunde des Jobcenters ist, da er die Miete selbst an den Vermieter zahlt.

Wir forderten den Vermieter zur Stellungnahme auf. Die Herkunft der Information, wonach der Petent Leistungsempfänger ist, ließ sich nicht mehr vollständig aufklären. Hinsichtlich der Datenübermittlung an das Jobcenter teilte uns der Vermieter mit, dass diese erfolgt sei, da das Jobcenter im Falle einer leer stehenden Wohnung die schon geleistete Miete zurückfordern würde. Aus Gründen der Schadensminderung sei deshalb eine Mitteilung an das Jobcenter erfolgt.

Bei der Information, dass eine bestimmte Person eine Wohnung vermutlich nicht mehr bewohnt, handelt es sich um ein personenbezogenes Datum im Sinne der datenschutzrechtlichen Vorschriften. Die Übermittlung dieser Information an das Jobcenter war schon deshalb nicht erforderlich und damit unzulässig, weil der Petent seine Miete regelmäßig selbst an den Vermieter überwies. Somit war keine Zahlungseinstellung durch das Jobcenter zu befürchten. Zudem durfte der Vermieter nicht automatisch davon ausgehen, dass der Mieter zum aktuellen Zeitpunkt noch Leistungen des Jobcenters bezog. Wir forderten deshalb den Vermieter auf, künftig keine personenbezogenen Daten mehr an das Jobcenter zu übermitteln und die Information, dass der Petent Leistungsempfänger sei, aus seinen Unterlagen zu löschen. Der Vermieter bestätigte uns, unseren Forderungen nachgekommen zu sein.

10. Wirtschaft und Häfen

10.1 Veröffentlichung von personenbezogenen Daten durch die Bremer Touristik Zentrale

Im Berichtsjahr bat uns die Bremer Touristik Zentrale (BTZ) um Beratung hinsichtlich der Veröffentlichung von Fotos, Videos und Panoramen im Internet. Die BTZ stellt auf ihrer Internetseite vielfältige Informationen für Touristinnen und Touristen zur Verfügung. Auf der Seite werden auch Fotos und Videos veröffentlicht, auf denen Bürgerinnen und Bürger zu erkennen sind. Hierbei stellt sich die Frage, ob und in welchem Umfang die Veröffentlichung solcher Aufnahmen zulässig ist.

Wir wiesen die BTZ darauf hin, dass eine Veröffentlichung von personenbezogenen Daten im Internet eine besondere Gefahr für das Recht auf informationelle Selbstbestimmung der Betroffenen darstellt, denn Informationen im Netz können weltweit beliebig abgerufen, verknüpft, weitergeleitet, kopiert und ausgewertet werden. Einmal im Internet vorhanden, lassen sich Daten kaum wieder zuverlässig daraus entfernen. Insofern hat eine Veröffentlichung im Internet eine andere Qualität als beispielsweise in Printmedien, von denen nur eine begrenzte Auflage existiert. Verschärft wird die Problematik durch neue technische Entwicklungen wie zum Beispiel Gesichtserkennungssoftware, mit deren Hilfe einzelne Personen gezielt identifiziert werden können.

Vor diesem Hintergrund ist eine Veröffentlichung personenbezogener Daten im Internet nur dann zulässig, wenn entweder eine Rechtsgrundlage dies erlaubt oder die Betroffenen ihre Einwilligung dazu erteilt haben. So dürfen beispielsweise Fotos veröffentlicht werden, die extra für diesen Zweck mit Hilfe von Fotomodellen angefertigt werden. Sollen Aufnahmen von Örtlichkeiten angefertigt werden, an denen sich Personen zufällig aufhalten und sind diese Personen auf den Aufnahmen identifizierbar, müssen sie um Erlaubnis gefragt werden, ob sie mit einer Veröffentlichung im Internet einverstanden sind. Auf der sicheren Seite befindet sich die veröffentlichende Stelle dann, wenn das Einverständnis schriftlich vorliegt. Sofern das Einholen einer Einwilligung nicht möglich ist, können die Aufnahmen dennoch veröffentlicht werden, wenn die Gesichter der Betroffenen unkenntlich gemacht werden oder durch Kunstgesichter ersetzt werden können.

Die BTZ sagte zu, diese Grundsätze bei neuen Aufnahmen zu berücksichtigen und im zweiten Schritt bereits vorhandene kritische Aufnahmen zu überarbeiten.

11. Finanzen und Verwaltungsmodernisierung

11.1 Berechnung der Pensionsrückstellungen im Rahmen der Eröffnungsbilanz

Im letzten Tätigkeitsbericht berichteten wir über ein bei der Senatorin für Finanzen angesiedeltes Projekt zur Berechnung der Pensionsrückstellungen im Rahmen der Eröffnungsbilanz, dessen Ziel die transparente Ausweisung der Vermögenslage der Freien Hansestadt Bremen ist. Grundlage der Kalkulation sind personenbezogene Daten der Mitarbeiterinnen und Mitarbeiter der Freien Hansestadt Bremen. Die eingesetzten Daten wurden weitestgehend anonymisiert. Bei Vorlage des letzten Tätigkeitsberichts war noch das für das Verfahren zu erstellende Datenschutzkonzept unvollständig. Es fehlte eine Beschreibung der technischen und organisatorischen Maßnahmen, die das Bremische Datenschutzgesetz zwingend fordert. Die genannten Maßnahmen sollen garantieren, dass ein sicherer Umgang mit den personenbezogenen Daten erfolgt. So müssen beispielsweise Vorkehrungen getroffen werden, damit Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen haben und Daten nicht unberechtigt gelesen, kopiert, geändert oder entfernt werden können. Die Verfahrensbeschreibung für die Anwendung Pensionsrückstellung wurde um die erforderlichen Angaben ergänzt.

Wir haben allerdings in diesem Zusammenhang festgestellt, dass für diese und weitere Auswertungen Daten aus bestehenden Personalverarbeitungssystemen exportiert und weiter verarbeitet werden. Zwar findet die Verarbeitung in der beim Referat 32 der Senatorin für Finanzen eingerichteten geschützten Informationstechnologie-Umgebung statt, dennoch aber entsprechen die dafür eingesetzten Anwendungen nicht dem Stand der Technik, so dass die Kontrollziele des Bremischen Datenschutzgesetzes nicht vollständig gewährleistet werden können. Wir haben die Senatorin für Finanzen aufgefordert, die Exporte im Rahmen der Weitergabekontrolle in den Quellsystemen zu protokollieren und zu dokumentieren, den Umfang der durchgeführten Auswertungen zu ermitteln und darzulegen sowie das Schutzniveau durch ergänzende Maßnahmen zu erhöhen. Die derzeitige Art der Verarbeitung stellt aus unserer Sicht lediglich eine Übergangslösung dar. Wir empfehlen dringend, die Auswertungen in die bestehenden Datenbanken zu integrieren und bei den Planungen für zukünftige Personalverarbeitungssysteme zu berücksichtigen.

11.2 Einrichtung einer zentralen Zuwendungsdatenbank

Auch im aktuellen Berichtsjahr wurde bei der Senatorin für Finanzen das Projekt zur Einrichtung einer zentralen Zuwendungsdatenbank weiter betrieben. Die Zu-

wendungsdatenbank soll dazu dienen, Mehrfachförderungen durch zuwendungsgebende Stellen zu verhindern, Transparenz zu schaffen und die Erstellung des jährlichen Zuwendungsberichtes zu vereinfachen. Bereits im letzten Jahresbericht erwähnten wir die Notwendigkeit, das Datenschutzkonzept im Rahmen des Projekts fortzuschreiben (vergleiche 33. Jahresbericht, Ziffer 10.2). Im April des Berichtsjahres wurde uns mitgeteilt, dass es im Projekt zu Verzögerungen gekommen sei, die sich auch auf die Erstellung des Datenschutzkonzeptes ausgewirkt hätten. Im September 2011 fand ein gesondertes Treffen mit Vertreterinnen und Vertretern der Senatorin für Finanzen und der Landesbeauftragten für Datenschutz und Informationsfreiheit statt, um den weiteren Projektverlauf und einzelne datenschutzrechtliche Anforderungen zu besprechen.

Aus Sicht des technischen und organisatorischen Datenschutzes sind die Vorgaben der §§ 7 und 8 Bremisches Datenschutzgesetz (BremDSG) zu beachten. Bezüglich der Gewährleistung der Kontrollziele haben wir unter anderem auf die sichere verschlüsselte Übertragung von personenbezogenen Daten, auf die Erstellung eines geeigneten Rechtekonzeptes und Rollenkonzeptes sowie auf die datenschutzgerechte Gestaltung der Historisierung und Protokollierung hingewiesen.

Vor dem Hintergrund der geschilderten Verzögerung des Projektes und da mögliche Szenarien der Bearbeitung von Anträgen noch nicht vollständig entschieden sind, ist auch eine weitere Stellungnahme zur Zuwendungsdatenbank im Moment nicht möglich; im Folgenden ein Beispiel:

Da neben den zuwendungsgewährenden Stellen auch fachliche Daten (zum Beispiel Prüfung von Bauzeichnungen, Ergebnisse fachtechnischer Prüfungen) gespeichert werden sollen, ist eine differenzierte Gestaltung der Berechtigungen erforderlich, wenn die fachtechnische Stelle hier selbst als Nutzerin des Systems auftreten will. Eine Problematik könnte dann beispielsweise in der datenschutzkonformen Gestaltung von Zugriffen auf importierte Dateien liegen. Werden neben personenbezogenen Daten wie zum Beispiel Stellenplänen auch fachtechnische Unterlagen importiert, auf die ein anderer Personenkreis Zugriff haben muss, so ist eine Trennung der Zugriffsmöglichkeiten auf diese beiden Bereiche notwendig, die es derzeit in der von uns angestrebten Form nicht gibt. In diesem Zusammenhang sind außerdem noch organisatorische Maßnahmen zu definieren. Es muss vorab sichergestellt werden, dass grundsätzlich nur die Daten importiert werden, die zur Aufgabenerfüllung erforderlich sind.

Weiteren Klärungsbedarf haben wir außerdem zum dargestellten Umfang der lesenden Zugriffe, der Gestaltung der Suchfunktion, zur revisionssicheren Speicherung administrativer Arbeiten und Zugriffe, dem Versand von Daten per E-Mail sowie dem geplanten Umfang der Exportfunktionen. Neben der grundsätzlichen Fortschreibung der Verfahrensbeschreibung erwarten wir zu den angesprochenen Themen ergänzende Angaben, um möglichst bald eine datenschutzrechtliche und datenschutztechnische Bewertung vornehmen zu können.

Sollte in einem späteren Stadium des Projektes eine Anbindung an das Internet erfolgen, so ist ein eigenes Sicherheitskonzept mit detaillierter Maßnahmenbeschreibung vor der Realisierung zu erstellen. Der Einsatz von Verschlüsselungsverfahren, Maßnahmen zur sicheren Authentifikation am System, eine sichere Überprüfung der Identität der Antragstellerinnen und Antragsteller sowie Maßnahmen zur Abschottung gegenüber Angriffen aus dem Internet sind erforderlich.

Sofern die Daten im Rahmen einer Auftragsdatenverarbeitung verarbeitet werden, ist diesbezüglich § 9 BremDSG zu beachten. Auch hier erwarten wir die erforderlichen Unterlagen.

Wir werden das Projekt auch weiterhin begleiten, um eine datenschutzkonforme Ausgestaltung der Zuwendungsdatenbank sicherzustellen.

11.3 Telefonisches BürgerServiceCentrum/D115

Das bei der Senatorin für Finanzen angesiedelte Projekt „Telefonisches Bürger ServiceCentrum/D115“ wird von uns weiterhin begleitet (siehe 33. Jahresbericht, Ziffer 10.4). Ziel des Projekts ist es, Bürgerinnen und Bürgern, die sich mit einem Anliegen an die bremische Verwaltung wenden, einen besseren Service zu bieten und die Voraussetzungen eines Beitritts zum D115-Verbund zu schaffen. Am 1. März 2011 startete das Bürgertelefon in Bremen mit der Telefonnummer 115. Uns wurde zu dem Verfahren ein Datenschutzkonzept vorgelegt, zu dem wir Stellung genom-

men haben. Wir hatten zu dem Konzept noch einige Fragen und Anmerkungen, zu denen uns die Performa Nord in der Zwischenzeit ein ausführliches Schreiben zukommen ließ. Derzeit ist unter anderem die Anforderung an die Eingabekontrolle nach § 7 Absatz 4 Satz 5 Bremisches Datenschutzgesetz noch nicht hinreichend erfüllt. Weiterhin sehen wir Klärungsbedarf bei der Versendung von Tickets innerhalb des Bremer Verwaltungsnetzes. Hier sehen sowohl das Bremische Datenschutzgesetz wie aber auch die bremische Richtlinie für die Nutzung der elektronischen Post eine Verschlüsselung von Personendaten vor. Darüber hinaus liegt uns derzeit kein Vertrag für diese Auftragsdatenverarbeitung vor. Unsere Anforderungen und Bedenken haben wir der Performa Nord erneut vorgetragen.

12. Medien

12.1 Datenschutz als Bildungsaufgabe

Viele gesellschaftliche und persönliche Aktivitäten finden im Internet statt. Besonders viele Kinder und Jugendliche nutzen das Internet zur privaten Kommunikation. Wegen der vielfältigen Risiken für das informationelle Selbstbestimmungsrecht der Nutzerinnen und Nutzer muss diesen Risiken entgegengewirkt werden. Die Datenschutzbeauftragten des Bundes und der Länder halten es für unabdingbar, den Datenschutz auch als Bildungsaufgabe zu verstehen und zu praktizieren. Daher hat ihre Konferenz eine entsprechende Entschließung (siehe Ziffer 20.9 dieses Berichts) gefasst.

12.2 Bremische Medienkompetenz

Im Berichtsjahr fand die Auftaktveranstaltung des von der Senatskanzlei einberufenen Runden Tisches zur Bremer Medienkompetenz statt. Ziel war es, die vielen bereits in Bremen existierenden Angebote zum Thema Medienkompetenz miteinander zu vernetzen. Gemeinsam ist den bremischen Angeboten, dass sie den kompetenten und qualifizierten Umgang mit Medien für eine der wichtigsten Fähigkeiten halten, um an der gesellschaftlichen und demokratischen Entwicklung teilzuhaben, und demzufolge die Vermittlung und das Erlernen von Medienkompetenz als eine zentrale Aufgabe ansehen, um allen Bevölkerungsgruppen diese Teilhabe zu ermöglichen. Im Rahmen der Auftaktveranstaltung stellten die Akteure, darunter auch die Landesbeauftragte für Datenschutz und Informationsfreiheit, ihre Aktivitäten und Schwerpunkte zur Medienkompetenz vor. Nach der Bildung von Arbeitsgruppen wurde ein Eckpunktepapier erstellt, das unter www.medienkompetenz.bremen.de abrufbar ist. Danach müssen die Rahmenpläne für die Schulen beständig fortgeschrieben und erneuert werden. Hierbei halten wir es insbesondere für dringend notwendig, den Rahmenplan Medienkompetenz aus dem Jahr 2002 an die neuen Anforderungen der Informationsgesellschaft anzupassen. Schwerpunkte müssen die Medienkompetenz im Rahmen der Persönlichkeitsentwicklung zu selbstbewussten Trägerinnen und Trägern von Grundrechten wie dem informationellen Selbstbestimmungsrecht und die Verarbeitung personenbezogener Daten im Internet, insbesondere in sozialen Netzwerken, sein. Wichtig ist natürlich auch, dass diese Rahmenpläne dann in der Schulpraxis umgesetzt werden.

In der Arbeitsgruppe „Alles legal?“ haben wir an der Beantwortung von Fragen zu rechtlichen Regelungen im Internet mitgearbeitet. Aus dieser Arbeitsgruppe ist dann eine öffentliche Veranstaltung zum Safer Internet Day 2011 hervorgegangen. Auf der Veranstaltung referierten Vertreterinnen und Vertreter der Bremischen Landesmedienanstalt, des Zentrums für Medien des Landesinstituts für Schule, der Verbraucherzentrale, der Polizei sowie der Landesbeauftragten für Datenschutz und Informationsfreiheit zu ihren fachspezifischen Themen.

Der Runde Tisch zur Bremer Medienkompetenz war ein guter Schritt in Richtung Vernetzung, weil sich viele Akteurinnen und Akteure im Bereich der Medienkompetenz kennengelernt haben. Nun gilt es, die Thematik zu vertiefen.

12.3 Runder Tisch Digitale Kultur und Schule

Seit mehreren Jahren trifft sich der Runde Tisch Digitale Kultur und Schule, um sich über Themen der Medienkompetenz auszutauschen. Mitglieder sind Vertrete-rinnen und Vertreter des Zentralelternbeirats, der Kooperationsstelle Universität – Schule, des Zentrums für Medien des Landesinstituts für Schule, einiger Schu-

len und des Jugendressorts sowie des Bildungsressorts und der Bremischen Landesmedienanstalt. In einer der letzten Sitzungen wurde sehr intensiv und kontrovers darüber beraten, ob beispielsweise das soziale Netzwerk facebook trotz seiner datenschutzrechtlichen Mängel im Unterricht eingesetzt werden darf. Wir wiesen dabei nachdrücklich darauf hin, dass der Anspruch der Vermittlung von Medienkompetenz für Schülerinnen und Schüler nicht mit dem Einsatz von datenschutzwidrigen Internetdiensten vereinbar ist.

Im September 2011 hat die Kooperationsstelle Universität–Schule einen Medienfachtag für Lehrkräfte, Eltern und sonstige Interessierte ausgerichtet. In verschiedenen Kursen wurden Themen zur Medienkompetenz bearbeitet, beispielsweise Spurensuche in den sozialen Netzwerken, Medienkompetenz und Computerführerschein, Lernen und Leben mit Medien sowie Elternarbeit zum Thema Internet und Schule.

12.4 Datenschutzerklärungen im Internet

Wir erhalten viele Eingaben zu mangelhaften Datenschutzerklärungen im Internet. Die datenschutzrechtlichen Vorgaben im Telemediengesetz legen fest, dass die Anbieter von Internetseiten die Nutzerinnen und Nutzer über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten informieren müssen. Oft sind diese Informationen nicht ausreichend oder nur schwer auf der Internetseite aufzufinden. Ein besonderes Problem stellen die Erhebung und Speicherung von Internetprotokoll-Adressen sowie die Gestaltung der eindeutigen und bewussten Einwilligung zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten dar. Viele Internetseitenbetreiber sind sich ihrer Pflichten als Anbieter nicht bewusst und vertrauen auf das rechtmäßige Verhalten ihrer technischen Dienstleister. Die datenschutzrechtlich verantwortliche Stelle bleibt jedoch die Betreiberin beziehungsweise der Betreiber der Internetseite, der somit auch die Einhaltung aller datenschutzrechtlichen Vorgaben – gegebenenfalls auch durch einen Dienstleister – sicherzustellen hat.

12.5 Nutzung von Web 2.0 durch öffentliche Stellen

Nicht nur eine große Anzahl privater Nutzerinnen und Nutzer, sondern zunehmend auch öffentliche Stellen halten soziale Netzwerke, Twitter, Blogs & Co für attraktiv. Die sogenannten Web-2.0-Technologien werden zur Außenkommunikation mit Bürgerinnen und Bürgern genutzt. Die Vorteile scheinen klar auf der Hand zu liegen: direkter Kontakt auch zu jüngeren Bürgerinnen und Bürgern. Informationen können schneller verbreitet werden, neue Vorhaben, Projekte oder aktuelle Themen können direkt diskutiert, Veranstaltungen beworben und Stimmungen eingeholt werden. Diesen möglichen Vorteilen ist entgegenzuhalten, dass der Umgang mit personenbezogenen Daten bei Web-2.0-Technologien immer wieder Grund zu starker Kritik ist. Die konkreten Ausgestaltungen dieser Technologien entsprechen oft nicht den Anforderungen des deutschen und europäischen Datenschutzrechts (siehe Ziffer 1.2 dieses Berichtes).

In diesem Jahr standen hauptsächlich soziale Netzwerke, insbesondere facebook, im Fokus der Aufsichtsbehörden. Viele bremische Stellen betreiben eine facebook-Fanpage und einige wenige hatten zusätzlich den „Gefällt-mir"-Button von facebook in ihren Internetauftritt integriert. Letzterer wurde von allen Stellen, nachdem sie von uns über die Funktionen informiert worden waren, entfernt.

Als verantwortliche Stelle und Diensteanbieter nach dem Telemediengesetz müssen Fanpage-Betreiber ihren Pflichten nachkommen. Nach dem Bremischen Datenschutzgesetz ist verantwortliche Stelle jede öffentliche Stelle, die personenbezogene Daten für sich selbst verarbeitet oder dies durch andere im Auftrag vornehmen lässt. Nach dem Telemediengesetz ist Diensteanbieter jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt. Fanpage-Betreiber nutzen die technische und organisatorische Infrastruktur von facebook und pflegen und gestalten den Inhalt der Fanpage. Insofern unterscheidet sich die Sachlage kaum von dem Betreiben eines eigenverantwortlich inhaltlich administrierten Internetauftritts. Damit sind Fanpage-Betreiber Diensteanbieter und datenschutzrechtlich verantwortliche Stellen.

Wir haben die Senatorin für Finanzen auf die Entschließung aufmerksam gemacht, die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ih-

rer Sitzung am 28. und 29. September 2011 in München zum Datenschutz in sozialen Netzwerken (vergleiche Ziffer 20.12 dieses Berichts) gefasst hat. Darin werden die öffentlichen Stellen aufgefordert, es zu verhindern, dass Bürgerinnen und Bürger, die sich auf den Seiten öffentlicher Stellen informieren wollen, damit mit ihren Daten bezahlen. Auch werden die öffentlichen Stellen aufgefordert, auf solchen Plattformen keine Profilseiten oder Fanpages einzurichten. Die Senatorin für Finanzen hat ein Schreiben an facebook versendet, das das Unternehmen auffordert, die Mängel im Hinblick auf den Datenschutz umgehend zu beseitigen. Das Unternehmen facebook hat darauf reagiert und ein Treffen mit der Senatorin für Finanzen angekündigt. Sollten die Betreiber von facebook keine dem Datenschutzrecht genügenden Anwendungen zur Verfügung stellen können oder wollen, hat die Senatorin für Finanzen zugesagt, dass die bremischen Fanpages auf Grund datenschutzrechtlicher Mängel abgeschaltet werden. Diese Zusage hat auch die Kriminalpolizei Bremerhaven in einem persönlichen Gespräch getätigt, sodass die Fahndungsseite, die gegenwärtig bei facebook betrieben wird, in diesem Fall abgeschaltet werden soll.

12.6 15. Rundfunkänderungsstaatsvertrag

Der 15. Rundfunkänderungsstaatsvertrag wurde nach der Unterzeichnung durch die Ministerpräsidentinnen und Ministerpräsidenten der Länder im Monat Dezember 2010 im laufenden Jahr 2011, den Landesparlamenten zur Beschlussfassung vorgelegt. In Bremen geschah dies schon Anfang des Jahres und aufgrund der Diskontinuität der Legislaturperioden erneut im August 2011. Die Bremische Bürgerschaft überwies den Gesetzesantrag nach der ersten Lesung zur Beratung und Berichterstattung an den Ausschuss für Wissenschaft, Medien, Datenschutz und Informationsfreiheit.

Kern des Rundfunkänderungsstaatsvertrags ist die Ablösung der bisherigen an den Besitz eines Empfangsgeräts gekoppelten Rundfunkgebühr durch die Erhebung eines an das Innehaben einer Wohnung oder einer Betriebsstätte angeknüpften Beitrages. Neben einer höheren Beitragsgerechtigkeit wird damit auch das Ziel einer deutlich datenschutzgerechteren Beitragserhebung verfolgt (siehe 33. Jahresbericht, Ziffer 11.2). Die Landesbeauftragten für Datenschutz hatten bereits im Vorfeld der Unterzeichung ausführlich die umfangreichen Erhebungsbefugnisse der Rundfunkanstalten kritisiert; leider wurden diese Kritikpunkte nur in sehr geringem Ausmaß ausgeräumt. Besonders die Beschaffung von Adressdaten aus privaten Quellen durch öffentliche Stellen wurde immer wieder als unverhältnismäßig bemängelt. Diese Befugnis ist im aktuellen Vertrag nicht komplett untersagt, sondern nur bis zum 31. Dezember 2014 ausgesetzt. Andere datenschutzrechtliche Forderungen sind in dem Vertrag selber unberücksichtigt geblieben, in einigen Bundesländern aber in Protokollerklärungen beziehungsweise durch Entschließungen, die Landtage begleitend zur Ratifizierung des 15. Rundfunkänderungsstaatsvertrages gefasst haben, vermerkt. In einem Gespräch zwischen Vertreterinnen und Vertretern der Rundfunkanstalten und den Aufsichtsbehörden, an dem auch die Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen beteiligt war, konnten zusätzlich Eckpunkte für eine Konkretisierung der datenschutzrechtlichen Anforderungen im Vollzug des 15. Rundfunkänderungsstaatsvertrag entworfen werden. Hierunter fallen neben der Konkretisierung von Erhebungsbefugnissen zum Beispiel auch die Verpflichtung, die Betroffenen darüber zu informieren, welche Quellen durch Rundfunkanstalten abgefragt werden, die Beschränkung der Nachweispflicht bei Abmeldung oder bei Beitragsbefreiungen auf die tatsächlich benötigten Daten sowie die Zugriffsbegrenzungen der Rundfunkanstalten auf ihre eigenen Datenbestände. Es ist dringend zu empfehlen, dass diese Eckpunkte verbindlich werden. In Betracht käme hierfür die noch zu erlassenden Satzungen der einzelnen Rundfunkanstalten.

12.7 Bericht aus dem Arbeitskreis Medien

Der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und die Arbeitsgruppe Telekommunikation, Teledienste und Mediendienste des Düsseldorfer Kreises tagten in diesem Jahr gemeinsam.

Im rein öffentlichen Bereich lag der Fokus auf dem 15. Rundfunkänderungsstaatsvertrag sowie auf den polizeilichen Ermittlungsbefugnissen in sozialen Netzwerken (siehe Ziffer 5.8 dieses Berichts und die Entschließung vom 29. September 2011, Ziffer 20.12 dieses Berichts; vergleiche 33. Jahresbericht, Ziffer 5.18).

Im gemeinsamen (öffentlichen und nicht-öffentlichen) Bereich wurden schwerpunktmäßig die Themen der Verarbeitung personenbezogener Daten in sozialen Netzwerken (insbesondere bei facebook, siehe Ziffer 12.6 dieses Berichts), die datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internetangeboten (insbesondere Google Analytics, eine Anwendung, die zur Analyse von Zugriffen auf Webseiten eingesetzt wird) sowie die anstehende Novellierung des Telemediengesetzes (TMG) behandelt.

Der Austausch im rein nicht-öffentlichen Bereich beinhaltete die datenschutzrechtliche Zulässigkeit der Verarbeitung von Funkzellendaten und Daten aus drahtlosen lokalen Netzwerken (WLAN), den datenschutzkonformen Einsatz von Smartphones sowie die Forderung nach anonymen und pseudonymen Zahlungsverfahren für Telemedien.

12.8 Datenschutzkolumne auf www.bremen.de

Seit Oktober 2011 veröffentlicht die Landesbeauftragte für Datenschutz und Informationsfreiheit eine Datenschutzkolumne auf www.bremen.de. Die Beiträge behandeln alle sechs Wochen aktuelle Themen rund um den Datenschutz. In den ersten beiden Ausgaben wurden unter der Internetadresse www.bremen.de/datenschutzkolumne Fragestellungen rund um das Recht am eigenen Bild und die Veröffentlichung von Fotos im Internet sowie die Datenschutzrisiken bei einer Mitgliedschaft bei facebook und das Betreiben einer Fanpage in dem sozialen Netzwerk behandelt.

13. Beschäftigtendatenschutz

13.1 Öffentlicher Bereich

13.1.1 Versendung von Höhergruppierungsanträgen und fristloser Kündigung per E-Mail

Ein Personalrat fragte uns, ob Höhergruppierungsanträge und Gründe, die dagegen sprechen, unverschlüsselt per E-Mail versandt werden dürfen. Gründe, die für oder insbesondere gegen Höhergruppierungsanträge genannt werden, sind häufig in der Person liegende Umstände, (beispielsweise deren Arbeitsleistung). Aber auch wenn die Gründe nur in der Bewertung des Arbeitsplatzes liegen aber einen Bezug auf einzelne Beschäftigte ermöglichen, handelt es sich um sensible Personaldaten. Ähnlich war der Fall, in dem eine Fachbereichsverwaltung der Hochschule Bremen mehrere wissenschaftliche Hilfskräfte über ihre fristlosen Kündigungen unverschlüsselt per E-Mail unterrichtet hatte. Auch diese Personaldaten sind zweifellos sensibel.

In beiden Fällen haben wir über die in der bremischen Verwaltung geltende E-Mail-Richtlinie unterrichtet, wonach sensible Daten mittels E-Mail nur unter Einsatz geeigneter Verschlüsselungsverfahren übermittelt werden dürfen. Die Hochschule hat daraufhin mitgeteilt, es habe sich um einen einmaligen Vorgang gehandelt. Sie habe diese Problematik mit den Beschäftigten der Fachbereichsverwaltung durchgesprochen und diese auf die E-Mail-Richtlinie hingewiesen.

13.1.2 Urlaubsgenehmigungen in offenen Postfächern der Raumpflegerinnen

In der Hochschule Bremen wurden Urlaubsgenehmigungen in offene Postfächer der Raumpflegerinnen gelegt, auf die auch andere Personen als die jeweils Betroffene zugreifen konnten. Unbeteiligte erhielten dadurch Kenntnis über Urlaubsgenehmigungen, Bildungsurlaube und Sonderurlaube aus besonderem Anlass wegen der Pflege einer oder eines Angehörigen. Die Hochschule teilte auf unseren Hinweis hin mit, zukünftig derartige Unterlagen in verschlossenen Briefumschlägen zu hinterlegen.

13.1.3 Empfangsbestätigung und Lesebestätigung von E-Mails

Eine Anfrage betraf das Aktivieren der Empfangsbestätigung und Lesebestätigung von E-Mails. Derartige Bestätigungen können zur Kontrolle der Beschäftigten verwendet werden. In diesem Fall haben wir auf die für die bremische Verwaltung geltende E-Mail-Richtlinie verwiesen. In dieser ist geregelt, dass nur im Bedarfsfall im versandten Nachrichtentext eine Empfangsbestätigung durch die Empfän-

gerin oder den Empfänger erbeten oder die Sendeoption eingestellt werden kann. Welcher Fall als Bedarfsfall angesehen kann, ist jedoch unklar. Die Absendung einer E-Mail, bei der keine Rückmeldung über die Nichtzustellbarkeit oder Abwesenheit beziehungsweise Weiterleitung erfolgt, gilt als in den Verfügungsbereich der Empfängerin oder des Empfängers gelangte Nachricht. Damit ist das Dokument als versandt und empfangen anzusehen. Es ist in der Regel unbedeutsam, zu welchem Zeitpunkt die Empfängerin oder der Empfänger eine Nachricht eingesehen beziehungsweise zur Kenntnis genommen hat.

Nachteilig beziehungsweise als belastend wird häufig empfunden, wenn Absendende regelmäßig eine Empfangsbestätigung verlangen, weil insoweit unterstellt würde, die Absendenden misstrauten der Empfängerin oder dem Empfänger und gingen davon aus, dass diese die E-Mail ohne Empfangsbestätigung nicht bearbeiten würde. Aus datenschutzrechtlicher Sicht kann die Nutzung der Sendeoption Empfangsbestätigung nur in einem begründeten Einzelfall erforderlich sein; eine regelmäßige Einstellung dieser Option ist nicht zulässig.

13.1.4 Internet-Recherchen über Polizeibedienstete

Auf Anfrage hat die Polizei Bremen erklärt, grundsätzlich würden keine Internet-Recherchen über Polizeibewerberinnen und Polizeibewerber sowie Polizeibedienstete durchgeführt. In Ausnahmefällen würden behauptete Fähigkeiten oder Eigenschaften einer Bewerberin oder eines Bewerbers nachgeprüft. Zu diesem Zweck würden Informationen aus dem Internet zu Rate gezogen. Behaupte beispielsweise eine Bewerberin oder ein Bewerber, sie oder er sei für den Polizeidienst besonders geeignet, weil sie oder er einen Meistertitel in Karate erworben habe, könnte eine einzelfallbezogene Recherche im Internet erfolgen. Die für den Polizeidienst ausgewählten Bewerberinnen und Bewerber würden darüber unterrichtet.

Daraufhin haben wir die Polizei Bremen auf den Grundsatz der Direkterhebung bei den Betroffenen hingewiesen. Es reicht regelmäßig aus, sich entsprechende Nachweise vorlegen zu lassen, beispielsweise die Urkunde über den Meistertitel in Karate, soweit dieser Nachweis tatsächlich erforderlich ist. Abgesehen davon bedeuten Internet-Recherchen zu einer bestimmten Person, dass regelmäßig Informationen erhoben werden, die die private Lebensgestaltung der oder des Betroffenen berühren. Diese Daten sind für die Bewerberauswahl nicht erforderlich.

Darüber hinaus können durch diese Recherchen schutzwürdige Belange der Betroffenen beeinträchtigt werden. Dem angehenden Dienstherrn würden Daten zur Kenntnis gelangen, die eine Benachteiligung nach dem Allgemeinen Gleichbehandlungsgrundsatz bedeuten können oder besondere Arten von Daten sind, beispielsweise Gesundheitsdaten, Gewerkschaftszugehörigkeit oder politische Überzeugungen. Diese Daten sind nicht für die Begründung oder Durchführung eines Beschäftigungsverhältnisses erforderlich.

Die Polizei Bremen hat uns zugesichert, zukünftig erfolge keine Datenerhebung über Polizeibewerberinnen und Polizeibewerber sowie Polizeibedienstete aus dem Internet. Sofern Daten gespeichert worden seien, würden diese unverzüglich gelöscht.

13.1.5 Datenverarbeitung bei einer Türschließanlage

Bei der Ortspolizeibehörde Bremerhaven wurde eine elektronische Türschließanlage installiert. Hierbei wurde drei Monate lang gespeichert, welche beziehungsweise welcher Beschäftigte an welchem Tag zu welcher Uhrzeit welche Tür geöffnet beziehungsweise geschlossen hat. In der Verfahrensbeschreibung wurde festgelegt, dass personenbezogene Auswertungen über die Türbewegungen nur zulässig sind, wenn sie zweckmäßig und erforderlich sind. Insbesondere sollten dadurch strafrechtliche oder disziplinarrechtliche Untersuchungen gefördert werden, soweit der Direktor der Ortspolizeibehörde zuvor zugestimmt hat.

Wir haben dargelegt, dass gerade der genannte Zweck eine als rechtswidrig zu qualifizierende Datenvorratspeicherung ist, die die Beschäftigten einem Generalverdacht aussetzt. Insoweit überwiegen die schutzwürdigen Belange der Beschäftigten. Daher haben wir gefordert, eine solche Auswertbarkeit auszuschließen, indem etwa die Daten automatisch nach einem Tag gelöscht werden.

Die Behördenleitung hat entschieden, keine Namen zu erfassen und diese durch eine Zahl zu ersetzen, sodass nunmehr lediglich eine anonymisierte Speicherung

erfolgt. Alle bisher erfassten Daten seien gelöscht worden. Dieser Vorgang zeigt einmal mehr, dass häufig die gesetzlich vorgeschriebene Vorabkontrolle nicht hinreichend erfolgt.

13.1.6 Namen und Namenskürzel über Lehrkräfte auf ausgehängten Stundenplänen und im Internet

Wir erhielten Hinweise, dass in praktisch allen Schulen ausgehängte Stundenpläne Namen oder Namenskürzel der jeweiligen Lehrkräfte enthalten. Da Schulen allgemein zugänglich sind, könnten dadurch regelmäßig andere Personen als Schülerinnen und Schüler sowie Lehrkräfte, diese Personaldaten zur Kenntnis nehmen, obwohl dies nicht erforderlich ist. Besonders gravierend ist es beispielsweise, wenn Stunden ausfallen und darauf geschlossen werden kann, welche Lehrkraft – aus welchen Gründen auch immer – abwesend ist. Auch im Internet wurden derartige Aushänge veröffentlicht.

Auf Anfrage hat das Bildungsressort mitgeteilt, es halte die Angabe der Namen oder Namenskürzel auf Aushängen und im Internet nicht für erforderlich und hat die Schulen angewiesen, auf diese Angaben in den Aushängen in der Schule zu verzichten. Die Veröffentlichung im Internet wird unterbleiben.

13.1.7 Bericht aus dem Arbeitskreis Personalwesen

Einmal jährlich tagt der Arbeitskreis Personalwesen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Im Berichtsjahr wurden insbesondere die Neuordnung des Beamtenrechts, automatisierte Personalverfahren im Bund und in den Ländern sowie das bundeseinheitliche polizeiliche Bewerberauswahlverfahren erörtert. Außerdem wurde über die Auswirkungen des Gesetzentwurfs zum Beschäftigtendatenschutz auf die Beamtengesetze sowie über das elektronische Entgeltnachweisverfahren ELENA und die Verfassungsklage dazu beraten.

13.2 Nicht-öffentlicher Bereich

13.2.1 Aktueller Stand zur Schaffung gesetzlicher Regelungen über den Beschäftigtendatenschutz im Bundesdatenschutzgesetz

In unserem letzten Jahresbericht haben wir unter den Ziffern 1.2 und 12.5 über den Gesetzentwurf der Bundesregierung und unsere Kritik daran berichtet. Der Gesetzentwurf soll gegenüber der bisherigen Regelung des § 32 Bundesdatenschutzgesetz weiter gefasste Regelungen zum Beschäftigtendatenschutz enthalten. Leider bleibt der Gesetzentwurf weit hinter dem in der arbeitsgerichtlichen Rechtsprechung entwickelten datenschutzrechtlichen Schutzniveau zurück. Unser Bericht endete damit, dass die Senatskommissarin für den Datenschutz unsere Änderungsvorschläge in den Bundesrat einbrachte und von dort eine Vielzahl übernommen wurde. Leider hat die Bundesregierung in ihrer Erwiderung zu dem Beschluss des Bundesrats praktisch alle Vorschläge zurückgewiesen.

Ende Mai 2011 fand im Innenausschuss des Bundestags eine öffentliche Anhörung zu dem Regierungsentwurf sowie den Gesetzentwürfen der Fraktionen der Sozialdemokratischen Partei Deutschland (SPD) und Bündnis 90/Die Grünen statt. In der öffentlichen Anhörung äußerten viele Sachverständige Kritik an dem Regierungsentwurf. Die Vertreterin des Deutschen Gewerkschaftsbundes monierte, der Regierungsentwurf entspreche nicht den Anforderungen an einen modernen Arbeitnehmerdatenschutz und werde den Abhängigkeiten im Arbeitsverhältnis nicht gerecht. Der Vertreter der Deutschen Vereinigung für Datenschutz bezeichnete die sogenannte Einwilligungsfreiheit des Beschäftigten als unrealistisch. Es gebe in der Arbeitswelt keine Verfügungsgewalt der oder des einzelnen Beschäftigten über ihre oder seine personenbezogenen Daten. Dies liege an dem Abhängigkeitsverhältnis der Beschäftigten im Arbeitsleben. Außerdem wurde kritisierte, der Entwurf enthalte keine wirksamen Sanktionen zum Schutz der Beschäftigten.

Die SPD-Fraktion fordert strengere Regelungen zum Beschäftigtendatenschutz und gegen den Missbrauch persönlicher Daten. Nach ihrem Gesetzentwurf sollen Unternehmen stärker als bisher verpflichtetet werden, die Persönlichkeitsrechte ihrer Beschäftigten zu achten. Sie hält eine Ausweitung der Mitbestimmung bei der Erhebung, Speicherung und Verarbeitung von Beschäftigtendaten für erforderlich, ebenso die Stärkung der Individualrechte der Beschäftigten.

Die Fraktion Bündnis 90/Die Grünen will dem Umgang mit personenbezogenen Daten von Beschäftigten klare Grenzen setzen. Ihrem Gesetzentwurf zufolge sollen medizinische und psychologische Untersuchungen künftig nur unter der Voraussetzung zulässig sein, dass sie für die Sicherheit der Berufsausübung erforderlich ist. Eine Überwachung durch optische und andere elektronische Einrichtungen zur Leistungskontrolle und Verhaltenskontrolle soll nur in eng begrenzten Fällen erlaubt sein. Zugleich will sie den Schutz vor Überwachung mit optischen und elektronischen Geräten erweitern.

Die Vertreterinnen und Vertreter der Regierungsfraktionen halten trotz der Kritik in der öffentlichen Anhörung an den Text ihres Gesetzentwurfs fest.

Anfang November 2011 hat die Herbstkonferenz der Justizministerinnen und Justizminister erneut bekräftigt, eine umfassende Regelung des Beschäftigtendatenschutzes sei dringend erforderlich. Zum Gesetzentwurf der Bundesregierung verlangt die Konferenz ein hohes Maß an Transparenz. So sollten die Arbeitgeberinnen und Arbeitgeber verpflichtet werden, die Beschäftigten darüber zu unterrichten, welche Daten über sie erhoben und gespeichert worden sind. Dies gelte besonders für Beschäftigtendaten, die die Arbeitgeberinnen beziehungsweise Arbeitgeber bei Dritten erhoben haben. Außerdem seien anlasslose Screening-Verfahren zur Aufdeckung möglicher Verfehlungen von Beschäftigten im Gesetz auszuschließen. Solche Verfahren seien von vornherein auf Fälle zu begrenzen, in denen zu dokumentierende tatsächliche Anhaltspunkte für bereits begangene Straftaten vorliegen. Sie seien auf den erforderlichen Umfang zu begrenzen. Es seien klare Regelungen zu schaffen, welche die private Nutzung von Telekommunikationseinrichtungen vor unzulässigen Datenerhebungen schützten. Außerdem dürften die Beschäftigten nicht dazu verpflichtet werden, ein betriebsinternes Beanstandungsverfahren zu durchlaufen, bevor sie sich an die für den Datenschutz zuständigen Aufsichtsbehörden wenden.

Inzwischen ist informell bekannt geworden, dass das Bundesministerium des Innern Änderungen vorschlagen wird, die die Prioritätenliste von Vertreterinnen und Vertretern der Regierungsfraktionen und von den Koalitionsfraktionen befürwortete Änderungen beinhalten. Diese stellen weitere Verschlechterungen für den Beschäftigtendatenschutz dar. So soll beispielsweise das Bundesdatenschutzgesetz nicht gelten, soweit Daten Gegenstand sozialüblicher innerbetrieblicher Kommunikation sind. Damit dürfte die E-Mail-Kommunikation zwischen den Beschäftigten der Verfügungsgewalt der Arbeitgeberinnen beziehungsweise der Arbeitgeber unterliegen, was nicht vertretbar ist.

Eine weitere Änderung betrifft die neue Regelung, dass allgemein zugängliche Daten nicht mehr unmittelbar bei der Beschäftigten oder dem Beschäftigten erhoben werden müssen. Insoweit wird der bisherige Entwurf gestrichen, wonach keine Daten aus sozialen Netzwerken im Internet erhoben werden dürfen, die der elektronischen Kommunikation dienen.

Offensichtlich auf Wunsch der Arbeitgeberseite soll nun noch eine Regelung geschaffen werden, wonach Beschäftigtendaten für die Versendung von Informationen und Meinungen über politische und wirtschaftliche Themen an die und den Beschäftigen verarbeitet oder genutzt werden dürfen. Die geplante Neuregelung würde es den Arbeitgeberinnen und Arbeitgebern erlauben, ihren Beschäftigten ungefragt die arbeitgebernahe Zeitschrift „aktiv“ nach Hause zu schicken. Damit soll offensichtlich eine rechtswidrige Praxis legalisiert werden. Die damit verbundene Übermittlung der Namen und Privatanschriften der Beschäftigten durch Arbeitgeberinnen beziehungsweise Arbeitgeber an den Verlag dieser Zeitschrift ist seit Jahren immer wieder Anlass zu Beschwerden von Beschäftigten bei der Landesbeauftragten für Datenschutz und Informationsfreiheit. Die Beschäftigten könnten sich bei der jetzt beabsichtigten Regelung dagegen nur wenden, wenn sie widersprochen haben. Dass sich die oder der Beschäftigte trauen, ihr Widerspruchsrecht geltend zu machen, dürfte aufgrund ihrer Abhängigkeiten im Arbeitsverhältnis unwahrscheinlich sein.

Immerhin soll nunmehr wieder die direkte Anrufung der Aufsichtsbehörde ohne vorherige betriebsinterne Klärung gewährleistet werden.

Insgesamt entsprechen die geplanten Änderungen am ohnehin schon datenschutzrechtlich hochproblematischen Entwurf der Bundesregierung sehr deutlich den Interessen der Arbeitgeberinnen und Arbeitgeber und gehen noch ein weiteres Mal

zu Lasten der Rechte der Beschäftigten. So begrüßt der Bundesverband der Arbeitgeberverbände die vorgenannten Änderungsvorschläge ebenfalls.

Von Arbeitnehmerseite dürfte zu Recht deutlicher Widerspruch gegen die weitaus meisten Regelungen zu erwarten sein.

13.2.2 Zugriff auf das E-Mail-Postfach bei Abwesenheit

Immer wieder werden wir gefragt, unter welchen Voraussetzungen auf das E-Mail-Postfach bei Abwesenheit einer oder eines Beschäftigten zugegriffen werden darf. Zur Frage, ob Beschäftigte auf den Schutz des Fernmeldegeheimnisses verzichten können, verweisen wir darauf, dass es einen derartigen Verzicht rechtlich nicht gibt. Dieses besondere grundrechtlich geschützte Geheimnis ist im Telekommunikationsgesetz ausgestaltet und gilt hinsichtlich der privaten E-Mail-Nutzung. Eine Verletzung des Fernmeldegeheimnisses etwa durch einen Verstoß gegen das Telekommunikationsgesetz stellt einen Straftatbestand nach dem Strafgesetzbuch dar. Ein Verstoß liegt jedoch nicht vor, wenn eine Beschäftigte oder ein Beschäftigter ohne faktischen Zwang – also völlig freiwillig – einwilligt, dass eine oder ein von ihm ebenso freiwillig bestimmte Beschäftigte oder ein bestimmter Beschäftigter während der Abwesenheit auf das E-Mail-Postfach zugreifen kann.

Dies geschieht technisch in der Weise, dass die oder der Betroffene selbst die entsprechende Einstellung vornimmt. Jedenfalls darf weder direkt noch indirekt Einfluss auf die Entscheidung der Mitarbeiterin oder des Mitarbeiters genommen werden. Zudem sind die Beschäftigten darüber zu unterrichten, dass sie den Zugriff jederzeit ohne Angaben von Gründen wieder rückgängig machen können. Es muss zudem regelmäßig die Wahlmöglichkeit bestehen, einer oder einem bestimmten Beschäftigten den Zugriff zu gewähren oder nur die Abwesenheitsassistenz zu aktivieren, verbunden mit dem Hinweis, dass der Absender sich in dringenden Fällen an die Poststelle oder an eine Vertreterin oder einen Vertreter wenden mögen. Bei Vorliegen der Einwilligung trägt die oder der Betroffene die Verantwortung nur für die von ihr oder ihm erlaubte Einsichtnahme in das E-Mail-Postfach durch eine bestimmte Beschäftigte oder einen bestimmten Beschäftigten. Es obliegt der Arbeitgeberin oder dem Arbeitgeber, dies technisch sicherzustellen.

Ein solcher Abwesenheitshinweis an potenzielle Absenderinnen oder Absender dürfte den Arbeitsablauf in den Unternehmen in keiner Weise stören, sodass eine Einflussnahme der oder des Vorgesetzten, die Weiterleitung zu aktivieren, nicht erforderlich und damit nicht zulässig ist. Auch wenn die private E-Mail-Nutzung ausdrücklich verboten ist, sind diese Wahlmöglichkeiten geboten.

E-Mail-Postfächer enthalten häufig vertrauliche Informationen, die nicht unmittelbar dienstlich relevant sind, beispielsweise die Kommunikation mit der Personalvertretung oder dem betriebsärztlichen Dienst. Häufig kommunizieren Kolleginnen und Kollegen beispielsweise anlässlich von Terminabsprachen über private Angelegenheiten, die betrieblich praktisch nicht unterbunden werden können.

Soweit innerhalb eines Unternehmens Unklarheiten zu diesen Fragen bestehen, sollten diese in einer Betriebsvereinbarung klärend geregelt werden. Ist kein Betriebsrat vorhanden, kommt eine entsprechende betriebliche Anweisung in Frage. Bedeutsam ist jedenfalls, dass alle Beschäftigten auf die Vorgaben und ihre Rechte hinzuweisen sind.

13.2.3 Telekommunikationsregelungen und Medienregelungen für Beschäftigte und Studierende in der Jacobs University

Aufgrund von Eingaben überprüften wir die Regelung der Jacobs University, die auch die private Nutzung von Telekommunikation (E-Mail) und Telemedien (Internet) erlaubt. Unsere Überprüfung ergab, dass insbesondere Speicherungen und Auswertungen dieser Nutzung nicht näher beschrieben waren. Es war geregelt, dass Dateien und E-Mails, die gegen diese Richtlinien verstoßen, geprüft, verändert und gelöscht werden sollten. Die Beschäftigten und Studierenden hatten eine Erklärung zu unterzeichnen, dass sie diese Befugnisse erlauben.

Wir verlangten, die Richtlinien an das Telekommunikationsgesetz und das Telemediengesetz anzupassen. Erst nach mehreren Überarbeitungen konnte erreicht werden, dass die Richtlinien gesetzeskonform ausgestaltet wurden. So sind Protokolldaten – insbesondere die Internetprotokoll-Adressen – nun spätestens nach sieben Tagen zu löschen. Bei vorhersehbarer Abwesenheit soll die oder der abwesende

Beschäftigte die Abwesenheitsassistenz aktivieren, mit der auf die Abwesenheit hingewiesen und für dringende Fälle eine andere E-Mail-Adresse genannt wird. Bei unvorhergesehener und längerer Abwesenheit wird die Installation der Abwesenheitsassistenz durch die Vorgesetzte oder den Vorgesetzten veranlasst. Eine personenbezogene Auswertung der Nutzung der Telemedien wird nur für einen Zeitraum von maximal vier Wochen vorgenommen, wenn tatsächliche Anhaltspunkte für einen begründeten Verdacht einer der in den Richtlinien aufgelisteten unzulässigen Nutzungen vorliegen. Die oder der betriebliche Datenschutzbeauftragte wird in diesem Fall vorher informiert. Nach Abschluss der Maßnahme werden die Betroffenen hierüber benachrichtigt.

13.2.4 Videoüberwachung der Beschäftigten auf dem Flur eines Bürogebäudes

Im Bürogebäude eines Hafenumschlagsunternehmens waren auf einem Flur acht Videokameras installiert, die auch auf die Toiletteneingänge sowie die Eingänge zu den Sozialräumen und Büroräumen gerichtet waren. Wir erhielten dazu Hinweise, dass auch Aufzeichnungen über Beschäftigte vorgenommen worden seien.

Aufgrund unserer Anfrage erklärte das Unternehmen, es habe mehrere Diebstahlsvorfälle in dem Bürogebäude gegeben. Auf Anraten der Kriminalpolizei habe sich das Unternehmen für die Videoüberwachung außerhalb der Arbeitszeiten entschieden. Eine permanente Überwachung der Beschäftigten sei nicht beabsichtigt gewesen. Lediglich im Falle eines Vorfalls habe das Unternehmen im Rahmen der Datenspeicherung nachweisen wollen, wer in diesem Zeitraum die Räumlichkeiten betreten hat. Das Unternehmen hat nunmehr die Videokameras komplett abmontiert.

13.2.5 Detaillierte Auswertungen über die Trainingshäufigkeit von Beschäftigten

Ein Unternehmen kooperiert mit mehreren Fitness-Studios in Bremen und näherer Umgebung. Auf seiner Homepage bietet es potenziellen Arbeitgeberinnen und Arbeitgebern detaillierte Auswertungen über ihre Beschäftigten an. Dies ist datenschutzrechtlich unzulässig, wenn Arbeitgeberinnen beziehungsweise Arbeitgeber dadurch personenbezogene Beschäftigtendaten erhalten, die für eine Nachprüfung, ob und wie häufig ihre Beschäftigten dort trainieren, und wie hoch die durch das Unternehmen dafür zu entrichtende Zahlung dementsprechend ausfällt, nicht erforderlich sind.

Das Unternehmen hat auf Anfrage erklärt und anhand von Unterlagen belegt, dass die Informationen für die Arbeitgeberinnen und Arbeitgeber keinen Bezug auf einzelne Beschäftigte aufweisen. In den Statistiken wird lediglich ausgewiesen, in welchen Studios wie viele Beschäftigte einer Arbeitgeberin beziehungsweise eines Arbeitgebers in bestimmten Zeiträumen trainieren. Den Beschäftigten stehe es frei, jederzeit das Fitness-Studio im Kooperationsverbund zu wechseln. Das Unternehmen ist unserer Aufforderung gefolgt und stellt auf seiner Homepage nun klar, dass nur anonymisierte Auswertungen vorgenommen werden.

In den Fällen, in denen die Arbeitgeberinnen und der Arbeitgeber Informationen über von ihnen mitfinanzierte Besuche von Beschäftigten in Fitness-Studios zur Berechnung des steuerrechtlich notwendigen individuellen geldwerten Vorteils benötigen, haben wir Folgendes vorgeschlagen: Das Unternehmen unterrichtet die Betroffenen vorher darüber, dass die für diesen Zweck erforderlichen Daten an die Arbeitgeberinnen beziehungsweise den Arbeitgeber übermittelt werden. Damit sollen die Betroffenen Gelegenheit erhalten, der Datenübermittlung zu widersprechen und die Angaben beispielsweise durch Vorlage einer Bescheinigung des Fitness-Studios selbst ihren Arbeitgeberinnen oder Arbeitgebern mitzuteilen. Darüber hinaus haben wir das Unternehmen gebeten, die Arbeitgeberinnen und Arbeitgeber auf ihre Unterrichtungspflichten gegenüber ihren Beschäftigten hinzuweisen. Das Unternehmen hat zugesagt, diese Vorgaben vollständig umzusetzen.

14. Auskunfteien

14.1 Bericht aus der Arbeitsgemeinschaft Auskunfteien

Auch im Berichtsjahr kamen die Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich wieder in der Arbeitsgemeinschaft Auskunfteien zusammen, um angesichts der im Bundesdatenschutzgesetz bestehenden Auslegungsspielräume eine über die Grenzen der Bundesländer hinausreichende einheitliche Rechtsauslegung

und Rechtsanwendung bei auskunfteienspezifischen Fragestellungen zu fördern. Nach wie vor werfen die durch den Gesetzgeber im Zuge der Novellierung des Bundesdatenschutzgesetzes eingeführten neuen Rechtsvorschriften Fragen auf, die erneut diskutiert wurden. Erörtert wurde daneben insbesondere wieder die Frage der Zulässigkeit beziehungsweise Unzulässigkeit der Anforderung einer Personalausweiskopie, wenn Betroffene ihren datenschutzrechtlichen Anspruch auf Auskunft über die bei einer Auskunftei gespeicherten Daten zu ihrer Person geltend machen (vergleiche 33. Jahresbericht, Ziffer 13.1). Zweifellos müssen auch Auskunfteien sicherstellen, dass die Eigenauskunft nicht von Dritten dazu missbraucht wird, personenbezogene Daten anderer Personen unrechtmäßig in Erfahrung zu bringen. Dies rechtfertigt jedoch mitnichten die generelle Anforderung einer, zudem auch noch ungeschwärzten Kopie des Personalausweises. Eine einfache Kopie eines Personalausweises ist nämlich bereits kein taugliches Mittel zum Identifikationsnachweis. Auch andere gewichtige Gründe sprechen gegen die Zulässigkeit eines solchen generellen Verlangens. Wir werden weiterhin ein wachsames Auge auf die in diesem Punkt ausgeübte Praxis der in unserem Zuständigkeitsbereich ansässigen Auskunfteien haben und gegen gegebenenfalls eingerissene missbräuchliche Handhabungen vorgehen.

15. Videoüberwachung

15.1 Videoüberwachung durch Privatpersonen

Wie schon in den früheren Jahren waren wir auch im aktuellen Berichtsjahr intensiv damit beschäftigt zu prüfen, ob der Einsatz einzelner Videokameras den Voraussetzungen der Datenschutzgesetze entspricht, und die Einhaltung dieser gesetzlichen Vorschriften durchzusetzen. Bereits im vorhergehenden Jahresbericht berichteten wir über die zunehmende Videoüberwachung in den verschiedensten Bereichen. Auch in diesem Zeitraum gerieten in dieser Hinsicht weitere Branchen in unseren Fokus, was einerseits mit den deutlich gesunkenen Preisen derartiger Anlagen, andererseits auch mit der erhöhten Sensibilität und Aufmerksamkeit der Öffentlichkeit zusammenhängt. Diese Entwicklung ist als ein weiterer Schritt in Richtung einer immer engmaschiger werdenden Videoüberwachung zu werten. In diesem Zusammenhang sind auch die uns weiterhin zahlreich erreichenden Beschwerden von Bürgerinnen und Bürgern zu sehen, die sich durch von Nachbarinnen beziehungsweise von Nachbarn angebrachter Videotechnik beobachtet oder sogar verfolgt fühlen. Hierdurch sollen ungeliebte Nachbarn zumeist eingeschüchtert werden, weil ihnen beispielsweise vorgeworfen wird, Unrat über den Zaun zu werfen, den Vorgarten durch Hundekot zu verunreinigen oder das Auto zu beschädigen. Wir werden zuständigkeitshalber erst dann tätig, wenn durch die Kameras öffentlich zugänglicher Raum erfasst wird, wie Bürgersteige, öffentliche Straßen und Zuwegungen. Sofern solch öffentlicher Raum überwacht wird, fordern wir diejenigen, die solche Kameras betreiben, auf, die Überwachung zu beenden. Da es sich um eine unzulässige Erhebung von personenbezogenen Daten handelt, kann ein Bußgeldverfahren eingeleitet werden. Sind die Kameras jedoch offensichtlich nur auf das eigene Grundstück ausgerichtet, können wir die Bürgerin beziehungsweise den Bürger nur auf den Zivilrechtsweg verweisen. Das Bundesdatenschutzgesetz ist in diesen Fällen nicht anwendbar, da die Datenverarbeitung nur zu persönlichen oder familiären Zwecken erfolgt und die Schlichtung privater Streitigkeiten nicht zu unserem Aufgabenbereich zählt.

Auch in diesem Jahr wollen wir nachfolgend aus den fast wöchentlich eingehenden Eingaben im Videoüberwachungsbereich einige Beispielsfälle näher darstellen.

15.2 Videoüberwachung im ECE-Einkaufszentrum

Das Unternehmen ECE betreibt als Eigentümer und Verwalter in Deutschland mehrere Einkaufszentren. Bei einer Überprüfung durch einige Datenschutzaufsichtbehörden wurde festgestellt, dass große Teile der Ladenpassagen mit Videokameras überwacht werden. Dabei gibt es Bereiche, deren Überwachung als erforderlich und zulässig angesehen werden kann, aber auch Bereiche, in denen dies problematisch ist. Videoüberwachung in Einkaufszentren ist nicht grundsätzlich unzulässig. Zu klären ist jedoch im Einzelfall, in welchen Bereichen eine Videoüberwachung tatsächlich erforderlich und geeignet ist, um mit der Videoüberwachung beabsichtigte gesetzmäßige Ziele zu erreichen und ob keine überwiegenden schutzwürdigen Interessen von Kundinnen, Kunden, Mitarbeiterinnen und Mitarbeitern

entgegenstehen. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit bearbeitete die Angelegenheit federführend, da sich der Sitz des Unternehmens ECE in Hamburg befindet und Umfang und Ausgestaltung der Videoüberwachung in den einzelnen Einkaufszentren auf Vorgaben und Entscheidungen des Unternehmens beruhten.

Letztlich kam der Hamburgische Datenschutzbeauftragte zu dem Ergebnis, dass die Interessen der Besucherinnen und Besucher, nicht ständig im Einkaufszentrum von einer Videoüberwachung erfasst zu werden, die Interessen des ECE an einer störungsfreien Atmosphäre überwiegen. Demzufolge wird das Unternehmen ECE in seinen deutschen Einkaufszentren die Videokameras in den Ladenpassagen größtenteils abbauen. Es wurde zwischen dem Hamburgischen Datenschutzbeauftragten und ECE Einigkeit darüber erzielt, welche Kameras abzubauen sind. An folgenden Standorten wurden die Kameras als grundsätzlich unzulässig angesehen: Fahrstühle, Fahrtreppen, Geldautomaten, Gastronomiebereiche inklusive Verweilzonen, Laufwege inklusive Verweilzonen, Toiletten, Toilettenzugänge und Umkleidebereiche. Das Ergebnis dieser Absprache wurde uns in einer von Hamburg übersandten Tabelle mitgeteilt. Hierin wurden alle in Frage kommenden Standorte von Videokameras mit einem Kommentar zur Notwendigkeit des Abbaus aufgelistet. Dies bildet die Grundlage für unsere Prüfung des bremischen ECE Einkaufzentrums. Hierbei wird von uns geprüft, ob die Absprachen mit der Datenschutzbehörde in Hamburg auch in Bremen entsprechend umgesetzt und die nicht für zulässig erachteten Kameras abgebaut wurden.

15.3 Videoüberwachung in Bäckereifilialen

Wir wurden darüber unterrichtet, dass in zwei Filialen einer Bäckerei mehrere Videokameras installiert seien. Auf unsere Anfrage hin erklärte uns das Unternehmens, dass die Kameras aufgrund von Einbrüchen eingebaut worden seien. In jeder Filiale seien sieben Kameras angebracht, die die Aufnahmen auch aufzeichnen würden. Die Kameras seien auf die Eingangstüren sowie die Kassen und Kleingeldtresore ausgerichtet und nur nach Geschäftsschluss aktiviert. Daraufhin erläuterten wir der Bäckerei, dass zwar aufgrund der geschilderten Übergriffe ein berechtigtes Interesse zur Installation der Kameras besteht, jedoch die Überwachung nach dem Gesetzeswortlaut auch erforderlich sein muss. Das bedeutet, sie muss zunächst überhaupt geeignet sein, den angestrebten Überwachungszweck zu erreichen und es ist zu prüfen, ob es nicht mildere, ebenfalls geeignete Mittel gibt. Im vorliegenden Fall reiche es daher zur Verhinderung von Einbrüchen völlig aus, nur den Bereich der Glasschiebewände nach Geschäftsschließung zu überwachen. Eine Überwachung der Kassen sowie der Kleingeldtresore ist für den von der Bäckerei festgelegten Zweck der Videoüberwachung zur Vermeidung von Einbrüchen, nicht erforderlich. Als milderes und ebenfalls geeignetes Mittel zur Sicherung der Kassen und Kleingeldtresore, könnten diese nach Geschäftsschluss geöffnet werden, wodurch offensichtlich erkennbar würde, dass sich kein Geld mehr darin befindet. Darüber hinaus wurde die Bäckerei aufgefordert einen betrieblichen Beauftragten für den Datenschutz zu bestellen sowie eine Verfahrensbeschreibung zu erstellen und uns zu erläutern, welche technischen und organisatorischen Maßnahmen ergriffen wurden, um die Videodaten vor unbefugten Zugriff zu schützen. Die Bäckerei bestätigte uns später, dass die Videoanlagen in beiden Filialen vollständig zurückgebaut worden seien.

15.4 Videoüberwachung eines öffentlich zugänglichen Arkadenganges

Im Berichtsjahr wurde an uns herangetragen, dass an den Hausfronten eines Bürogebäudes und Geschäftshauses Videokameras angebracht seien. Das Gebäude sei von allen Seiten von öffentlich zugänglichen Fußwegen umgeben, die direkt an die Hausfront angrenzen, wobei es sich auf zwei Seiten um Arkadengänge handelt, die parallel zu Straßen verlaufen. Es sei daher zu befürchten, dass durch die Ausrichtung der Kameras diese öffentlichen Bereiche überwacht würden. Durch die örtlichen Begebenheiten sei es Fußgängern nicht möglich, der Überwachung auszuweichen, da dies nur durch Überqueren von stark befahrenen Straßen zu realisieren sei. Nachdem wir bei der verantwortlichen Stelle angefragt hatten, wurde aufgrund dieser Stellungnahme umgehend ein Prüftermin vereinbart, um die Angelegenheit vor Ort in Augenschein zu nehmen. Hierbei konnten wir feststellen, dass die Beschreibung der örtlichen Situation zutraf. Die Fußwege sowie die Arkadengänge sind als öffentlich zugängliche Bereiche anzusehen, obwohl sich die-

se Flächen im Eigentum der verantwortlichen Stelle befinden. Aufgrund der vorgelegten Dokumente konnte die verantwortliche Stelle ihr berechtigtes Interesse an einer Videoüberwachung nachweisen. Diese ist aber nur im Rahmen der gesetzlich erlaubten Wahrnehmung des Hausrechts zulässig. Hierbei darf nur ein schmaler Bereich vor der Hausfront von den Kameras erfasst werden und somit nur noch Personen, die sich in unmittelbarer Nähe der Hausfassade befinden. Letztlich konnte dies gegenüber der verantwortlichen Stelle durchgesetzt werden. Sie hat uns bestätigt, dass während der Videoaufnahmen nunmehr eine automatisierte Schwärzung der Bereiche, die nicht die datenschutzrechtlich erlaubte Ausübung des Hausrechts betreffen, stattfinden würde. Diese Schwärzung der Aufnahmen könne auch nachträglich nicht wieder entfernt werden. Des Weiteren wurden die Verfahrenbeschreibung angepasst und deutlich sichtbare Hinweisschilder auf eine Videoüberwachung an den Gebäudeecken angebracht.

15.5 Videoüberwachung eines Studentenwohnheimes

Im Frühjahr dieses Jahres wurden wir von Bewohnerinnen und Bewohnern eines Studentenwohnheimes darauf hingewiesen, dass auf dem Gelände der Anlage damit begonnen worden sei, Videoüberwachungskameras anzubringen. Hierdurch sei zu befürchten, dass auch die zu den Wohnungen führenden Treppenhäuser, der Weg zu den Müllcontainern und der Rezeption sowie auf dem Gelände befindliche öffentliche Wege überwacht würden. Beängstigend sei auch der Umstand, dass die Kameras auf vor dem Gebäude befindlichen Masten installiert werden sollen. Somit sei nicht auszuschließen, dass die gesamte Gebäudefront einschließlich der sich in den oberen Etagen befindlichen Fenster der Räumlichkeiten der Bewohnerinnen und Bewohner von den Kameras erfasst würden. Auf unsere Anfrage hin teilte uns die verantwortliche Stelle mit, dass mit der Installation der Kameras noch nicht begonnen worden sei. Außerdem sei aufgrund unseres Anschreibens zwischenzeitlich ein externer Datenschutzbeauftragter beauftragt worden. Wir haben daraufhin mit dem Manager der Anlage sowie den externen Datenschutzbeauftragten einen Vororttermin vereinbart, um mit ihnen die weitere Vorgehensweise in dieser Angelegenheit zu besprechen, damit die Videoüberwachungsanlage den datenschutzrechtlichen Vorschriften entsprechend betrieben werden kann. Bei der durchgeführten Vorortbesichtigung wurden die einzelnen Kamerastandorte sowie deren Erfassungsbereiche abgesprochen. Sowohl der Manager als auch der Datenschutzbeauftragte folgten unseren Forderungen und bestätigten uns später schriftlich, dass die Umsetzung der von uns geforderten Maßnahmen erfolgt sei. Wir haben damit erreicht, dass weder die sich in den oberen Etagen befindlichen Wohnbereiche des Gebäudes, noch die weiteren oben angesprochenen Bereiche überwacht werden können. Dies wurde dadurch erreicht, dass bestimmte Teile des von der Kamera erfassten Bereichs dauerhaft und irreversibel geschwärzt werden. Außerdem wird die Videoüberwachung nur außerhalb der Bürozeiten der Rezeption durchgeführt. Die verantwortliche Stelle bestätigte, dass deutlich sichtbare Hinweisschilder an den abgesprochenen Stellen angebracht sowie eine Verfahrenbeschreibung erstellt worden seien, die die von uns geforderten Zusatzangaben hinsichtlich der Überwachungsbereiche enthalte.

15.6 Videoüberwachung des Betriebes sowie dazugehöriger Verkaufsräume und Restaurants eines Unternehmens

Im Berichtsjahr sind wir darauf aufmerksam gemacht worden, dass in einem Restaurant sowie in anderen Geschäftsräumen und Verkaufsräumen eines Unternehmens etliche Videokameras angebracht waren, die eine Überwachung von Beschäftigten, Gästen sowie Kundinnen und Kunden ermöglichten. Auf unsere Anfrage hin, bestätigte uns das Unternehmen die Installation von insgesamt mehr als dreißig Kameras. Aufgrund der Vielzahl von Kameras an den verschiedensten Standorten führten wir daraufhin eine Vorortprüfung durch, um die einzelnen Kameras in Augenschein zu nehmen. Das Unternehmen bestätigte uns schriftlich, dass die Umsetzung der von uns im Prüfbericht geforderten Maßnahmen erfolgt sei. In Bezug auf die im Produktionsbetrieb installierten Kameras erreichten wir, dass die Erfassungswinkel verschiedener Kameras angepasst wurden, um keine Mitarbeiterüberwachung zu ermöglichen. Außerdem konnten wir durchsetzen, dass die in diesem Bereich zur Einbruchsverhinderung innen angebrachten Kameras auf die Außenfassade des Gebäudes versetzt wurden. Hierdurch können potentielle Störerinnen oder Störer von der Videoüberwachung Kenntnis nehmen und werden durch die zusätzlich anzubringenden Hinweisschilder abgeschreckt. Bei den in den Ver-

kaufsräumen installierten Kameras wurden zwei Kameras unverzüglich abmontiert, da mit ihnen eine Mitarbeiterüberwachung möglich gewesen wäre. Ebenso wurden in den Verkaufsräumen sowie in den Restaurants die Einstellungen einzelner Kameras angepasst. Darüber hinaus findet in den Restaurants eine Aufzeichnung der Videobilder nur noch nach Geschäftsschluss statt.

15.7 Videoüberwachung der Hauseingänge und Fahrstühle in einer Wohnanlage

Mehrere Bewohner einer Wohnanlage beschwerten sich bei uns, dass die Hauseingänge und Fahrstühle durch Videokameras überwacht würden. Die verantwortliche Stelle beantwortete zwar unsere Anfrage, die Antworten ließen jedoch eine abschließende Beurteilung der Angelegenheit nicht zu, sodass wir auch in diesem Fall eine Vorortprüfung durchführten. Da es in der Wohnanlage in der Vergangenheit zu gravierenden und belegbaren Vorfällen in den Hauseingängen kam, bestand seitens der verantwortlichen Stelle ein berechtigtes Interesse an einer Videoüberwachung, denn eine andere Lösung zum Schutze der Bewohnerinnen und Bewohner war nicht ersichtlich. Aber auch in solch einem Ausnahmefall müssen Maßnahmen zur Wahrung der schutzwürdigen Interessen der Betroffenen und der Besucherinnen und Besucher getroffen werden. Eine Neuausrichtung der Kameras beseitigte in diesem Fall dieses Problem. Wir setzten dabei durch, dass nur noch die Eingangstüren von den Kameras erfasst werden und nicht wie zuvor der gesamte Eingangsraum einschließlich der Briefkästen. Darüber hinaus ist der Zugriffsschutz auf die gefertigten Aufnahmen verschärft worden, damit niemand ohne konkreten Anlass in die Daten einsehen kann. So können sich die Betroffenen nunmehr darauf verlassen, dass die Aufzeichnungen nicht dazu benutzt werden können, um Bewegungsprofile von ihnen zu erstellen. Die verantwortliche Stelle bestellt zudem einen betrieblichen Datenschutzbeauftragten. Bezogen auf die Kameras in den Fahrstühlen konnten uns schwerwiegende Beeinträchtigungen der Rechte der Hausbewohnerinnen und Hausbewohner, etwa Angriffe auf die Person oder ihrer unmittelbaren Wohnsphäre, nicht nachgewiesen werden. Letztlich sicherte uns die verantwortliche Stelle zu, dass die Kameras in den Fahrstühlen komplett abmontiert worden seien.

15.8 Bericht aus dem Arbeitskreis Steuerverwaltung

Die Landesbeauftragte für Datenschutz und Informationsfreiheit nahm an der Sitzung des Arbeitskreises Steuerverwaltung der Konferenz Datenschutzbeauftragten des Bundes und der Länder teil. Der Arbeitskreis dient dem Austausch von Erfahrungen und Informationen sowie einer möglichst einheitlichen Vorgehensweise in den teilnehmenden Ländern.

Im Berichtsjahr wurden unter anderem die folgenden Themen behandelt: Kontrollbefugnis der Datenschutzbeauftragten gegenüber der Steuerfahndung, Schwierigkeiten bei der Verwendung der Steuer-Identifikationsnummer, Evaluierungsbericht zum anderen sicheren Verfahren nach § 87 a Abgabenordnung, Folgen der dauerhaften Zulassung von ELSTER-Online (elektronische Steuererklärung), Auskunftsanspruch in der Abgabenordnung, ELStAM-Datenbank (elektronische Lohnsteuerabzugsmerkmale), Elektronische Lohnsteuerkarte, Kirchensteuer auf Kapitalerträge, Kontendatenabruf, Betriebsprüfung bei einer Steuerberatungsgesellschaft, Ankauf von Steuerdaten durch Finanzbehörden und Datenschutzaufsicht im Zusammenhang mit der Erhebung der Kraftfahrzeugsteuer.

16. Dienstleistungen

16.1 Werbung

Für Unternehmen im Markt sind Werbeansprachen ein Mittel, um den Absatz von Produkten oder Dienstleistungen sicherzustellen beziehungsweise zu verbessern. Auf Seiten der Verbraucherinnen und Verbraucher wird Werbung aber nicht nur als willkommenes Informationsangebot, sondern vielfach auch als unerwünschte Belästigung empfunden. Für Werbeansprachen bestehen daher rechtliche Vorgaben, insbesondere im Gesetz gegen den unlauteren Wettbewerb, aber auch im Bundesdatenschutzgesetz. Wie uns die Vielzahl der im Berichtsjahr eingegangen Beschwerden über Werbemaßnahmen beweist, werden diese rechtlichen Vorgaben seitens der Werbetreibenden jedoch nicht immer beachtet. Insbesondere im Bereich des Telefonmarketings tummeln sich zahlreiche schwarze Schafe. Eine Ahndung

begangener Datenschutzverstöße ist häufig aus praktischen Gründen nicht möglich, was auszugsweise die nachfolgenden Beispiele belegen.

Einige generelle Informationen zu den datenschutzrechtlichen Aspekten der Werbung, insbesondere auch zu den für Bürgerinnen und Bürger nach dem Bundesdatenschutzgesetz bestehenden Reaktionsmöglichkeiten auf unerwünschte Werbung, finden sich in der im Berichtsjahr in Zusammenarbeit verschiedener Datenschutzaufsichtsbehörden unter Federführung des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen überarbeiteten Broschüre „Bitte keine Werbung“. Die Broschüre ist über unsere Webseite unter http://www.datenschutz-bremen.de/tipps/adresshandel.php abrufbar.

16.1.1 Missachtung von Werbewidersprüchen

Wie erwähnt legt das Bundesdatenschutzgesetz unter anderem auch Anforderungen an die Verwendung persönlicher Daten für Werbezwecke fest. Es gewährt insoweit auch allen das Recht, der Verarbeitung oder Nutzung der eigenen Daten, etwa Adressdaten, für Zwecke der Werbung und Marktforschung oder Meinungsforschung zu widersprechen (sogenanntes Werbewiderspruchsrecht). Die Ausübung dieses Widerspruchsrechts gegenüber der werbenden Person beziehungsweise dem werbenden Unternehmen führt dazu, dass eine weitere Verwendung der persönlichen Angaben generell unzulässig wird. Der Werbende hat sicherzustellen, dass keine weiteren Werbeansprachen erfolgen. Damit dieses Werbewiderspruchsrecht Betroffenen zur Kenntnis gelangt, verpflichtet das Bundesdatenschutzgesetz Werbetreibende dazu, bei Werbeansprachen und gegebenenfalls bei einem Vertragsschluss auf das Werbewiderspruchsrecht hinzuweisen. Verstöße gegen diese Vorgaben stellen unter Umständen eine bußgeldbewehrte Ordnungswidrigkeit dar.

Gleichwohl wird diesen rechtlichen Vorgaben nicht immer in der gebotenen Weise Rechnung getragen. So beschwerte sich bei uns im Berichtsjahr beispielsweise ein Bürger – er hatte im Rahmen des Abschlusses eines Zeitschriften-Abonnementsvertrages zunächst in eine Werbeansprache eingewilligt, später aber künftiger Werbung nachweislich widersprochen – darüber, dass er trotz seines Werbewiderspruchs wiederholt Werbeanrufe des Unternehmens erhalten hätte. Wir wandten uns zur Klärung an das fragliche Unternehmen. Im Rahmen der Nachforschung zur Pannenursache stellte das Unternehmen fest, dass die Weitergabe des eingegangenen Werbewiderspruchs an das mit der Durchführung der Telefonwerbung beauftragte Call-Center beziehungsweise die dortige Eintragung des Werbewiderspruchs im Kundendatensatz unterblieben war. Grund hierfür war die Unaufmerksamkeit eines Mitarbeiters. Das Unternehmen reagierte unmittelbar und führte ein technisches Verfahren ein, das künftig die unmittelbare Berücksichtigung des Widerspruchs beim Telefondienstleister sicherstellt. Aufgrund dieser unmittelbaren Reaktion des Unternehmens bestand für uns kein Anlass zu weitergehenden Maßnahmen.

16.1.2 Unzulässige Telefonwerbeanrufe

Telefonwerbeanrufe waren wie schon in den vorhergehenden Berichten generell wieder Gegenstand zahlreicher Anfragen und Beschwerden auch in diesem Berichtsjahr. Einige Betroffene schilderten uns, dass sie an manchen Tagen, auch an Sonntagen und an Feiertagen, bis in die späten Abendstunden hinein unzählige Werbeanrufe unbekannter Unternehmen beziehungsweise Personen erhalten hätten. Ziel dieser Anrufe war und ist es regelmäßig, unter Ausnutzung des Überraschungsmoments mit geschickten Gesprächsstrategien die Angerufenen zu überrumpeln und zum Abschluss kostenpflichtiger Verträge, insbesondere über angebliche Lotteriedienstleistungen oder Gewinnspieldienstleistungen, zu drängen oder den Angerufenen vorzugaukeln, sie hätten einen Vertrag abgeschlossen und seien nun zahlungspflichtig. Rechtlich verstießen diese Anrufe mangels ausdrücklicher Einwilligung der Angerufenen in die telefonische Werbeansprache durchweg gegen das im August 2009 zwecks Bekämpfung der unangeforderten Telefonwerbung novellierte Gesetz gegen den unlauteren Wettbewerb. Die Bundesnetzagentur kann, sofern sich der Anrufer ermitteln lässt, solche unzulässigen Werbeanrufe im Wege einer Geldbuße sanktionieren. Zugleich verstießen diese Anrufe aber auch gegen die durch uns durchzusetzenden Maßgaben des Bundesdatenschutzgesetzes. Wir als Datenschutzaufsichtsbehörde stehen in diesen Fällen jedoch in der Regel vor dem praktischen Problem, dass die Anruferin oder der Anrufer mangels Namensnennung beziehungsweise Nennung eines falschen Namens nicht identifizierbar ist. Eine Rückverfolgung des Anrufs über die Rufnummer ist in diesen Fällen re-

gelmäßig ebenfalls nicht möglich. Entweder wird nämlich die Rufnummer unterdrückt, obwohl dies bei Werbeanrufen nach dem Telekommunikationsgesetz ausdrücklich verboten ist, oder es wird eine falsche Rufnummer im Telefondisplay angezeigt, was sich häufig bei Rückrufversuchen der oder des Betroffenen herausstellte. Telekommunikationstechnische Ermittlungsbefugnisse besitzen wir nicht, sodass wir die tatsächliche Rufnummer auch nicht ermitteln können. In einigen Fällen konnten Betroffene feststellen, dass die Werbeanrufe aus dem Nicht-EU-Ausland (EU steht für Europäische Union) stammten, was eine Rechtsdurchsetzung von vornherein faktisch aussichtslos macht. Praktisch können wir daher in diesen Fällen die Betroffenen bei der Durchsetzung ihrer datenschutzrechtlichen Rechte nicht unterstützen. Ein neuerliches gesetzgeberisches Tätigwerden, das nunmehr wirksam das Problem belästigender Telefonwerbung bekämpft, ist dringend erforderlich. Der Bundesrat hat im Juli 2011 als Reaktion auf die Problematik einen Gesetzentwurf in den Bundestag (Bundestags-Drucksache 17/6482) eingebracht, mittels dessen diese unseriösen Werbeanrufe eingedämmt werden sollen. Es bleibt abzuwarten, ob sich Bundestag wie Bundesregierung des hinreichend bekannten Problems annehmen.

16.1.3 Insbesondere Telefonwerbung für Datenlöschungsdienste im Internet

Bereits in unserem letzten Jahresbericht (siehe 33. Jahresbericht, Ziffer 15.2) berichteten wir ausführlich über die Abzock-Masche nicht näher bekannter Personen, die als angebliche Mitarbeiterinnen oder Mitarbeiter einer Datenschutzeinrichtung telefonisch Kontakt mit Bürgerinnen und Bürgern aufnahmen und anboten, gegen Entgelt – Entrichtung zumeist via Bankeinzug – für eine Löschung vermeintlich im Internet zirkulierender Daten der Angerufenen zu sorgen. Auch in diesem Jahr erhielten wir wieder Nachfragen zu derartigen Anrufen. In der Sache kann nach wie vor nur dringend empfohlen werden, auf solche Angebote nicht einzugehen. Ziel dieser Anrufe ist es wohl ausschließlich, die Gesprächspartner zur Mitteilung oder Bestätigung persönlicher Angaben, wie etwa Adressdaten oder insbesondere auch Bankverbindungsdaten, zu verleiten.

16.1.4 Unzulässige Werbeansprachen via E-Mail

Viele Beschwerden richteten sich auch in diesem Berichtsjahr wieder gegen Werbeansprachen via E-Mail, die häufig als Massen-Mails beziehungsweise Spam-Mails versandt werden. Bereits im letzten Jahresbericht berichteten wir exemplarisch über einen Fall (siehe 33. Jahresbericht, Ziffer 15.4). Die zum Versand benötigten E-Mail-Empfängeradressen werden häufig automatisch aus dem Internet, etwa Chat-Foren oder Webseiten, ausgelesen. Einige der uns seitens Betroffener vorgelegten Spam-Mails enthielten sogar einen Hinweis auf das Werbewiderspruchsrecht und benannten eine E-Mail-Adresse, an die ein etwaiger Werbewiderspruch gesandt werden sollte. Sandten die Betroffenen an diese E-Mail-Adresse allerdings einen Widerspruch, so erhielten sie in der Folge erst recht weitere Werbe-Mails; sie zeigten nämlich dem Versender – wie beabsichtigt –, dass ihre Mail-Adresse tatsächlich existiert und genutzt wird. Bei Spam-Mails ist eine Ermittlung der Urheberin beziehungsweise des Urhebers für uns ebenfalls regelmäßig praktisch ausgeschlossen. Den Werbewiderspruch der Betroffenen können wir daher auch in diesem Bereich faktisch nicht durchsetzen. Es empfiehlt sich daher, auf Spam-Mails nicht zu reagieren und durch Einstellung des Spam-Filters die belästigenden E-Mails automatisch aus der elektronischen Post aussortieren zu lassen.

16.1.5 Postalische „Gewinnmitteilungen“ und „Kaffeefahrten“

Zurückgegangen gegenüber dem Vorjahr war in diesem Berichtsjahr die Anzahl der im Zusammenhang mit einer postalischen vermeintlichen Gewinnmitteilung bei uns eingegangenen Beschwerden. Ob dies jedoch aus einem tatsächlichen Rückgang der „Kaffeefahrteinladungsschreiben und Gewinnmitteilungsschreiben“ oder lediglich aus gesunkener Beschwerdeneigung Betroffener resultiert, lässt sich nicht feststellen. In der Sache machten die Betroffenen nach Erhalt eines solchen Briefes zumeist ihr Recht auf Eigendatenauskunft (vergleiche Ziffer 16.2 dieses Berichts) geltend und baten um Datensperrung für Werbezwecke nebst Bestätigung dieser Sperrung. Eine Reaktion der sich zumeist mit Phantasiefirmen tarnenden und nur unter Postfachanschriften agierenden Postabsender erfolgte hierauf erwartungsgemäß nicht. Wie stets in diesen Fällen (vergleiche 33. Jahresbericht, Ziffer 15.4) stehen wir bei dem Versuch der Durchsetzung dieser datenschutzrechtlichen Betroffenenrechte vor dem Problem, dass die angeblichen Unternehmen nicht exis-

tieren und die dahinterstehenden Personen allenfalls durch Zufall ermittelbar sind. Immerhin konnten und können wir in diesen Fällen zumeist darauf hinwirken, dass das Postfach seitens des Postfach-Vermieters gekündigt wird. Die Problematik der fehlenden Möglichkeit des Vollzugs des Datenschutzrechts auch in diesem Bereich ist jedoch nach wie vor ungelöst.

16.2 Missachtung des datenschutzrechtlichen Eigenauskunftsanspruchs Betroffener

Das Bundesdatenschutzgesetz gewährt allen, deren persönliche Daten durch andere Personen oder Stellen automatisiert oder dateimäßig erhoben beziehungsweise verwendet werden, grundsätzlich einen Anspruch auf Auskunft,

— welche Daten zur Person im Einzelnen gespeichert sind,

— gegebenenfalls woher diese Daten stammen,

— an wen die Daten bereits weitergegeben wurden, beziehungsweise an wen sie noch weitergegeben werden sollen, und schließlich

— wozu diese Daten konkret gespeichert werden (sogenannte Selbstauskunft oder Betroffenen-Eigenauskunft).

Zum Teil verwenden Unternehmen, beispielsweise Banken und Telekommunikationsunternehmen, bei Geschäftsabschlüssen statistische Wahrscheinlichkeitswerte, die aus bereits vorhandenen persönlichen Daten errechnet werden und eine Aussage dazu ermöglichen sollen, ob eine Person als Vertragspartnerin beziehungsweise Vertragspartner auch zahlungsfähig und zahlungswillig ist (sogenannte Score-Werte). Im Falle des Einsatzes solcher Score-Werte erweitert sich der Eigenauskunftsanspruch: den Betroffenen ist dann zusätzlich zu den oben genannten Informationen insbesondere auch mitzuteilen, wie dieser Wahrscheinlichkeitswert aussieht, was er genau bedeutet und wie und mit welchen Datenarten er berechnet wurde. Der Auskunftsanspruch ist kostenlos. Wird den Anfragenden die Auskunft nicht, nicht richtig, unvollständig oder vorwerfbar verspätet erteilt, so stellt dies unter Umständen eine Ordnungswidrigkeit dar.

Die unzulängliche oder gar ausgebliebene Reaktion auf solche Auskunftserteilungsgesuche war auch in diesem Berichtsjahr wieder Gegenstand einiger Beschwerden bei uns. Exemplarisch seien folgende beiden Fälle erwähnt: Bei einem Unternehmen, das auf mehrfache Anfrage eines Betroffenen nicht reagierte, lag, wie oftmals in diesen Fällen, schlichtweg ein Organisationsmangel vor. Mitarbeiterinnen beziehungsweise Mitarbeiter der Marketing-Abteilung hatten die Auskunftsgesuche nicht an die für die Beantwortung zuständige Stelle des Unternehmens weitergeleitet. Selbstverständlich haben datenverarbeitende Stellen ihre interne Organisation so auszugestalten, dass die Beantwortung von Eigenauskunftsanfragen sichergestellt ist. Wir forderten das Unternehmen daher auf, die Prozesse so zu organisieren, dass künftig solche Fehler möglichst ausgeschlossen sind. Das Unternehmen kam dem umgehend nach, sodass insoweit kein weiterer Handlungsbedarf für uns bestand.

Nicht immer liegt die Ursache für eine ausbleibende Reaktion auf Auskunftsanfragen aber im Bereich der datenverarbeitenden Stelle. Dies zeigte sich in folgendem Fall: Der Betroffene hatte in Reaktion auf den Erhalt eines E-Mail-Newsletters zwar per E-Mail seinen Eigenauskunftsanspruch geltend gemacht, dabei aber über die Antwortfunktion des E-Mail-Programms die Newsletter-Absender-Adresse als Empfangsadresse seiner Mail gewählt. Aufgrund entsprechender Einstellung des E-Mail-Servers des Unternehmens wurden aber unter dieser Adresse keine E-Mails empfangen. Das Unternehmen wies hierauf in seinem Newsletter ausdrücklich hin und gab eine andere E-Mail-Adresse für die Kontaktaufnahme via elektronischer Post an. Da die oder der Auskunftssuchende nach allgemeinen Grundsätzen dafür Sorge zu tragen hat, dass ihre oder seine Erklärung im Rechtsverkehr der Empfängerin beziehungsweise dem Empfänger auch zugeht, war dem Unternehmen hier kein datenschutzrechtliches Fehlverhalten vorzuwerfen.

17. Kreditwirtschaft

17.1 Sichtschutz an Selbstbedienungsterminals der Kreditinstitute

Bereits in den beiden vergangenen Jahresberichten berichteten wir ausführlich darüber, dass einige Kreditinstitute bei der Auswahl und Aufstellung ihrer Über-

weisungsterminals beziehungsweise Zahlungsverkehrsterminals mitunter zu wenig Acht auf datenschutzrechtliche Anforderungen legten. Es gab bei den in dieser Hinsicht überprüften Kreditinstituten zumindest in einem Teil der Filialen beziehungsweise Gerätestandorte keine ausreichenden Vorkehrungen, um Kundinnen und Kunden hinreichend vor unbefugtem Mitlesen ihrer Eingaben durch Dritte zu schützen. Auf unsere Beanstandung hin reagierte eines der Kreditinstitute zügig, überprüfte die Situation bei allen Gerätestandorten und sorgte bei Feststellung entsprechender Mängel für Abhilfe, etwa indem Geräte anders ausgerichtet oder gänzlich anders platziert oder durch zusätzliche Trennwände vor Blicken Dritter abgeschottet wurden. Nach einer stichprobenweisen Überprüfung gehen wir nunmehr von einem hinreichenden Schutzniveau in den Filialen dieses Kreditinstituts aus.

Bei einem anderen Kreditinstitut, das zunächst in einer besonders betroffenen Filiale die Situation gut löste und auch nachfolgend an einigen anderen Standorten tätig wurde, verzögert sich nunmehr trotz mehrfacher Anmahnungen die Beseitigung der Mängel in weiteren Filialen erheblich. Das Kreditinstitut ist nunmehr der Auffassung, dass es datenschutzrechtlich nicht zur Herstellung eines ausreichenden Sichtschutzes verpflichtet sei. Abgesehen davon, dass wir diese Meinung für offenkundig rechtlich fehlerhaft halten und entsprechend auf eine Korrektur hinwirken werden, verblüfft auch die fehlende Sensibilität und Rücksichtnahme auf die schutzwürdigen Belange der Kundinnen und Kunden. Wir werden uns dieser Angelegenheit weiter annehmen und darauf hinwirken, dass bei den weiteren betroffenen Filialen beziehungsweise Gerätestandorten für hinreichenden Sichtschutz gesorgt wird.

17.2 Registrierung und Beaufsichtigung von Anlageberatern

Ein Mitarbeiter eines Kreditinstituts sah sich durch eine neue gesetzliche Regelung im Wertpapierhandelsgesetz in seinem Recht, über den Umgang mit seinen Daten selbst zu bestimmen, verletzt und wandte sich mit der Bitte um Rat und Unterstützung an uns. Anlass seiner Sorge war eine Vorschrift, die der Deutsche Bundestag im Februar 2011 im Zuge des „Gesetzes zur Stärkung des Anlegerschutzes und Verbesserung der Funktionsfähigkeit des Kapitalmarkts“ beschloss. Als Reaktion auf die im Rahmen der Finanzkrise gewonnenen Erkenntnisse des Gesetzgebers um die Notwendigkeit eines besseren Anlegerschutzes sollte mit den neuen Regelungen eine effektivere Kontrolle im Anlageberatungsgeschäft durch die Bundesanstalt für Finanzdienstleistungsaufsicht ermöglicht werden. Die seitens des Betroffenen monierte Vorschrift verpflichtet Banken und sonstige Finanzdienstleistungsinstitute, welche Wertpapierdienstleistungen erbringen, mit Wirkung ab November 2012 der Bundesanstalt für Finanzdienstleistungsaufsicht die in der Anlageberatung tätigen Mitarbeiterinnen und Mitarbeiter zu benennen. Zudem müssen der Bundesanstalt Beschwerden mitgeteilt werden, die beispielsweise seitens Kundinnen und Kunden über die einzelnen Anlageberaterinnen und Anlageberater eingegangen sind. Die mitgeteilten Anlageberaterdaten sowie gegebenenfalls die jeweiligen Kundenbeschwerdeanzeigen werden sodann zu Kontrollzwecken in einer internen Datenbank der Bundesanstalt für Finanzdienstleistungen gespeichert.

Da es sich um ein im Zeitpunkt der Anfrage bereits in Kraft getretenes Bundesgesetz handelte und wir als vollziehende Verwaltungsbehörde an die Gesetze gebunden sind, aber keine Befugnis zur verbindlichen datenschutzrechtlichen Überprüfung von Parlamentsgesetzen besitzen, verwiesen wir den Betroffenen auf die gesetzliche Lage. Allein das Bundesverfassungsgericht könnte hier im Falle der Feststellung einer Verletzung der Rechte von Personen, die in der Anlageberatung tätig sind, das Gesetz für verfassungswidrig erklären und damit die Mitteilungspflicht von Daten an die Bundesanstalt für Finanzdienstleistungen außer Kraft setzen.

17.3 Bericht aus der Arbeitsgruppe Kreditwirtschaft

Auch in diesem Berichtsjahr fand wieder die alljährliche Sitzung der Arbeitsgruppe Kreditwirtschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder statt. Diese dient der Koordinierung der Aufsichtspraxis gegenüber Kreditinstituten, da die Datenschutzaufsichtsbehörden als Landesbehörden jeweils eigenständig für die Überwachung der Einhaltung datenschutzrechtlicher Vorschriften in den Bundesländern zuständig sind. Themen der diesjährigen Sitzung waren unter anderem die Umsetzung der im Zuge der zurückliegenden Novellierung des Bundesdatenschutzgesetzes vorgenommenen gesetzlichen Änderungen durch die Kre-

ditinstitute, sodann die bereits in Presseberichten erwähnten Pläne der Sparkassen zur Einführung von Funkchips in den Eurochequekarten zwecks Erleichterung bargeldloser Zahlungen, des Weiteren das Verlangen einiger Kreditinstitute nach Vorlage von Kontoauszügen bei Kreditanträgen und die Sicherstellung der Rückabwicklung fehlgeleiteter Überweisungsbeträge.

Was bei Darlehensanträgen die Aufforderung gegenüber der oder des Kreditsuchenden zur Vorlage von Kontoauszügen zwecks Prüfung der Kreditwürdigkeit anbelangt, so müssen die Kreditinstitute die Kreditsuchenden – um eine Erhebung nicht erforderlicher Daten zu vermeiden – darauf hinweisen, dass alle nicht kreditrelevanten Angaben auf den Kontoauszügen geschwärzt werden dürfen. Es geht die Bank nämlich beispielsweise nichts an, ob die oder der Kreditsuchende Mitglied in einem Verein ist, bei welcher Krankenkasse sie oder er versichert ist und ähnliches. Derartige Informationen lassen sich dem Kontoauszug aber aufgrund der Abbuchungen und Buchungsnachweise ohne Weiteres entnehmen, mit der Folge, dass weitgehende Rückschlüsse auf die Lebensumstände der Kontoinhaberin oder des Kontoinhabers möglich sind.

Bei der Rückabwicklung fehlgeleiteter Überweisungen stellen sich ebenfalls datenschutzrechtliche Fragen. Die derzeitige zivilrechtliche Rechtslage lässt sich wie folgt skizzieren: Nach einer Vorschrift des Bürgerlichen Gesetzbuchs dürfen sich Banken und andere Zahlungsdienstleister bei der Ausführung von Überweisungen auf die angegebene „Kundenkennung“ der Zahlungsempfängerin beziehungsweise des Zahlungsempfängers, das heißt bei Überweisungen innerhalb Deutschlands üblicherweise: Kontonummer und Bankleitzahl der Empfängerin oder des Empfängers, verlassen. Die ehemals übliche Überprüfung, ob die angegebene Bankverbindung und Kontoverbindung auch der beziehungsweise dem namentlich benannten Zahlungsempfänger zugeordnet ist, unterbleibt. Laut amtlicher Gesetzesbegründung soll hiermit die Abwicklung des Zahlungsverkehrs beschleunigt werden. Kehrseite der Medaille ist das hiermit verbundene erhöhte Risiko von Fehlüberweisungen, da sich bei der Eingabe von vielstelligen Ziffernfolgen bei Kontonummer und Bankleitzahl leicht Fehler einschleichen. Fehler bei der Überweisung infolge unrichtig eingegebener Bankdaten der Zahlungsempfängerin beziehungsweise des Zahlungsempfängers gehen damit also allein zu Lasten der Zahlerin beziehungsweise des Zahlers. Ansprüche gegen die Bank oder den Zahlungsdienstleister auf Rückerstattung bestehen nicht. Der Gesetzgeber gesteht der beziehungsweise dem Überweisenden lediglich einen Anspruch darauf zu, dass sich die Bank beziehungsweise der Finanzdienstleister im Rahmen seiner Möglichkeiten darum bemüht, den Zahlungsbetrag wiederzuerlangen. Falls die Zahlungsempfängerin beziehungsweise der Zahlungsempfänger nicht bereits von sich aus eine Rückbuchung des fehlerhaft überwiesenen Betrags veranlasst, stellt sich datenschutzrechtlich die Frage, ob ihre beziehungsweise seine Bank unter Berufung auf den Datenschutz die Herausgabe des Namens und der Anschrift verweigern darf. Die Aufsichtsbehörden sind der einhelligen Auffassung, dass eine Rückabwicklung der Fehlüberweisung nicht unter Berufung der Empfängerbank auf datenschutzrechtliche Gründe erschwert oder vereitelt werden darf. Die oder der Überweisende hat hier einen Anspruch auf Auskunft hinsichtlich der Kontaktdaten der Zahlungsempfängerin beziehungsweise des Zahlungsempfängers. Allerdings muss sichergestellt sein, dass deren Daten erst dann an die oder den Überweisenden herausgegeben werden, wenn sie beziehungsweise er nicht kooperationswillig ist. Zudem muss dafür Sorge getragen werden, dass eine vorhergehende Information über solche Datenübermittlungen stattfindet.

18. Ordnungswidrigkeiten und Zwangsverfahren

18.1 Ordnungswidrigkeitsverfahren

Die Zahl der von uns im Berichtsjahr wegen des Verstoßes gegen das Bundesdatenschutzgesetz (BDSG) betriebenen Ordnungswidrigkeitsverfahren lag bei neun und hat sich damit im Vergleich zum Vorjahr nahezu verdoppelt, wobei die von den Verfahren betroffenen Sachverhalte unterschiedlicher Art waren. Mehrere Verfahren betrafen erneut die Nichterteilung von Auskünften an die Betroffenen oder an die Aufsichtsbehörde. Wegen der festgestellten Verstöße wurden von uns Bußgelder in Höhe von 800 Euro bis 1 600 Euro festgesetzt. Da in den betreffenden Fällen gegen die jeweiligen Bußgeldbescheide Einspruch eingelegt wurde und diesen wegen fehlender oder unzureichender Gründe nicht abgeholfen werden konnte,

wurden die Vorgänge zur weiteren Bearbeitung an die Staatsanwaltschaft abgegeben. Notwendige Verhandlungstermine vor dem Amtsgericht stehen zurzeit noch aus.

Gleich mit mehreren Verstößen gegen das Bundesdatenschutzgesetz verbunden war die Übermittlung einer hohen Zahl von Daten von Kundinnen und Kunden und Vereinsmitgliedern durch zwei wirtschaftlich miteinander verwobene Unternehmen im Sportbereich an eine Medienfirma zur Versendung eines Newsletters. Die Übermittlung sollte im Rahmen der Erteilung von Aufträgen zur Verarbeitung personenbezogener Daten erfolgen. Die Aufträge waren entgegen den Vorgaben des Bundesdatenschutzgesetzes jedoch weder richtig noch vollständig erteilt worden. Insbesondere mangelte es an der notwendigen Schriftform. Die bei einer Auftragsdatenverarbeitung festzulegenden Inhalte waren nicht in die Aufträge einbezogen worden. Auch der Verpflichtung, sich vor Beginn der Datenverarbeitung über die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen, waren die auftraggebenden Unternehmen nicht nachgekommen. Eine Überprüfung der Maßnahmen war nicht erfolgt. Diese Verstöße gegen das Bundesdatenschutzgesetz stellen eine Ordnungswidrigkeit dar. Gegen die Geschäftsführer der beiden Unternehmen wurden deshalb Ordnungswidrigkeitsverfahren durchgeführt und als deren Ergebnis Bußgeldbescheide erlassen, mit denen Bußgelder in Höhe von 5 000 Euro beziehungsweise 3 000 Euro verhängt wurden. Die Bußgelder wurden von den beiden Geschäftsführern bezahlt.

Ein weiterer Bußgeldverstoß betraf die unbefugte Erhebung und Verarbeitung personenbezogener Daten durch einen Mitarbeiter eines Kreditinstituts. Der Mitarbeiter fragte die Daten eines potenziellen Kunden bei der SCHUFA ab, ohne dass die hierfür erforderliche Einwilligung des Betroffenen vorlag. Bei der Bearbeitung des Vorgangs erklärte uns das Kreditinstitut, dass es seine Mitarbeiterinnen und Mitarbeiter immer wieder auf die bei SCHUFA-Abfragen zu beachtenden Regelungen hingewiesen habe, somit wies die Geschäftsführung des Kreditinstituts die Verantwortung von sich. Die unbefugte Erhebung und Verarbeitung personenbezogener Daten ist bußgeldbewehrt. Da davon auszugehen war, dass auch der betreffende Mitarbeiter des Kreditinstituts die bei SCHUFA-Abfragen zu beachtenden Bestimmungen kannte, wurde der Bescheid über ein Bußgeld in Höhe von 1 200 Euro gegen ihn erlassen. Gegen den Bescheid wurde Einspruch eingelegt. Da diesem nicht abgeholfen werden konnte, wurde der Vorgang zur weiteren Bearbeitung an die Staatsanwaltschaft abgegeben, ein Verhandlungstermin vor dem Amtsgericht Bremen steht zurzeit noch aus.

Ein weiterer Verstoß gegen das Bundesdatenschutzgesetz ergab sich im Hinblick auf die Übermittlung personenbezogener Daten durch einen Arzt an ein medizinisches Hochschulinstitut. Übermittelt wurden neben dem Namen und der Anschrift besonders sensible Daten über das Vorliegen einer Erkrankung, ohne dass hierfür die Einwilligung des betreffenden Patienten vorlag oder dass es hierfür eine Vorschrift gab, die die Übermittlung erlaubte. Gegen den Arzt verhängten wir ein Bußgeld in Höhe von 1 200 Euro, das dieser bezahlte.

Des Weiteren betrieben wir ein Ordnungswidrigkeitsverfahren wegen der unbefugten Bereithaltung personenbezogener Daten zum Abruf mittels automatisierten Verfahrens, was nach § 43 Absatz 2 Ziffer 2 BDSG eine Ordnungswidrigkeit darstellt. Ein Fotograf hatte auf einem Schulfest Fotos gemacht und diese auf der Internetseite seiner Firma für alle Internetnutzerinnen und Internetnutzer frei zugänglich veröffentlicht. Die Veröffentlichung war mit den Bestimmungen des Kunsturhebergesetzes, dessen Regelungen eine bereichsspezifische Sondervorschrift für Bildnisse als personenbezogene Daten darstellen, nicht zu vereinbaren. Auch lag die Einwilligung der Erziehungsberechtigten für die Veröffentlichung der Bilder nicht vor. Gegen den Fotografen wurde ein Bußgeldbescheid erlassen, der auch rechtskräftig wurde. Die Zahlung des festgesetzten Bußgeldes in Höhe von 1 800 Euro steht bislang aus.

18.2 Zwangsverfahren der Aufsichtsbehörde

Zur Durchsetzung datenschutzrechtlicher Anforderungen wurden auch im Berichtsjahr Zwangsgelder angedroht und festgesetzt. Angedroht wurden Zwangsgelder bis zu einer Höhe von 5 000 Euro, festgesetzt bis zu einer Höhe von 2 500 Euro, wobei ausschlaggebend für die Höhe des Zwangsgeldes jeweils die Bedeutung des Vorgangs war. Erneut war insbesondere die Nichterteilung von Auskünften Ge-

genstand. Bei zwei Vorgängen wurden wegen der Nichteinhaltung des Telemediengesetzes Zwangsgelder in Höhe von bis zu 1 000 Euro angedroht. Erneut gab es auch im Berichtsjahr einen Fall, bei dem die Festsetzung von nur einem Zwangsgeld nicht ausreichte. Das Verfahren gegen dieses Unternehmen dauert an.

19. Datenschutz auf europäischer und internationaler Ebene

19.1 Datenschutz in der Europäischen Union

In der Mitteilung der Kommission über ein Gesamtkonzept für den Datenschutz in der Europäischen Union (Kommissionsdokument 2010 [609]) vom 4. November 2010 wird ein Konzept für eine Reform der europäischen Rechtsordnung betreffend den Schutz personenbezogener Daten in allen Tätigkeitsbereichen der Europäischen Union vorgestellt. Insbesondere werden die Herausforderungen der Globalisierung und neuer Technologien berücksichtigt. Dieses Konzept fokussiert Änderungen der bisherigen Richtlinie 95/46/EG (Europäische Gemeinschaft) vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. In seiner Stellungnahme vom 12. Januar 2011 wird das reformierende Anliegen der Europäischen Kommission vom Europäischen Datenschutzbeauftragten grundsätzlich begrüßt. Auch das Europäische Parlament hat sich diesem Votum insgesamt angeschlossen und in seiner Entschließung vom 6. Juli 2011 die Mitteilung der Kommission unterstützt. Es wird mit Spannung der Vorschlag für eine neue europäische Rechtsordnung im Datenschutz, geplant für Januar 2012, erwartet, der auch Auswirkungen auf das deutsche Datenschutzrecht haben kann (vergleiche Ziffer 19.4 dieses Berichts).

19.2 Übermittlung massenhafter Zahlungsverkehrsdaten in die USA und das europäische „Terrorist Finance Tracking System“

In der Mitteilung der Europäischen Kommission zu Optionen für ein EU-System (EU steht für Europäische Union) zum Aufspüren der Terrorismusfinanzierung (Kommissionsdokument [2011] 429; Bundesratsdrucksache 415/11) wird das Ziel formuliert, ein System in der Europäischen Union zu schaffen, das die Übermittlung massenhafter Daten an die Vereinigten Staaten von Amerika (USA) nach dem sogenannten SWIFT-Abkommen (Society for Worldwide Interbank Financial Telecommunication) beziehungsweise TFTP-Abkommen beendet (vergleiche 33. Jahresbericht, Ziffer 18.4). TFTP bedeutet „Terrorist Finance Tracking Program“, was ein Programm zum Aufspüren der Finanzierung des Terrorismus beinhaltet. Die bestehenden datenschutzrechtlichen Bedenken gegen dieses Abkommen zwischen der Europäischen Union und den USA werden mit dem neuen, von der Europäischen Kommission geplanten Terrorist Finance Tracking System (TFTS) allerdings nicht ausgeräumt. Nach der Kommissionsmitteilung sollen durch das europäische TFTS einheitliche Regeln und datenschutzrechtliche Standards für die Extraktion von Zahlungsverkehrsdaten für die gesamte Europäische Union geschaffen werden. Ohne den Nachweis der Erforderlichkeit eines europäischen Systems zum Aufspüren von Terrorismusfinanzierung kann aus datenschutzrechtlicher Sicht die Einführung eines europäischen Systems nicht begrüßt werden. Das TFTS stellt eine Vorratsdatenspeicherung dar, wogegen wir grundsätzliche Bedenken haben. Ungeachtet des neuen TFTS fordern wir weiterhin, die Übermittlungen massenhafter Zahlungsverkehrsdaten in die USA nach dem SWIFT-Abkommen zu be-enden.

19.3 Bericht aus der Arbeitsgruppe Internationaler Datenverkehr

Die Landesbeauftragte für Datenschutz und Informationsfreiheit nahm an der dem Erfahrungsaustausch und Informationsaustausch dienenden Arbeitsgruppe Internationaler Datenverkehr der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich teil. Im Berichtsjahr hat sich die Arbeitsgruppe mit den folgenden Themen beschäftigt:

— Verbindliche Unternehmensregelungen für Auftraggeber und neu für Auftragnehmer,

— Abgleich der Terrorlisten der Europäischen Union bei der Anerkennung des AEO (Authorized Economic Operators)-Status,

— Virenfilterung und Spamfilterung als Auftragsdatenverarbeitung,

— Datentransfer über einen Router mit Standort im Drittstaat,

— Übermittlung besonderer Arten von personenbezogenen Daten zum Zweck der Auftragsdatenverarbeitung in Drittstaaten mit angemessenem Datenschutzniveau und Cloud Computing.

19.4 Bericht aus dem Arbeitskreis Europa

Im Mittelpunkt der Arbeit des Arbeitskreises Europa der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Berichtsjahr stand die Revision der europäischen Datenschutzrichtlinie (siehe Ziffer 19.1 dieses Berichts). Ziel ist es, das Datenschutzrecht in Europa zu vereinheitlichen. Die Überarbeitung der europäischen Datenschutzrichtlinie wird derart gestaltet sein, dass sowohl eine unmittelbar geltende Verordnung als auch eine umsetzungsbedürftige europäische Richtlinie als Rechtsinstrumente eingesetzt werden. Inhaltlich soll die europäische Datenschutzverordnung folgendes regeln: Sofern Unternehmen in mehreren Mitgliedstaaten tätig sind, soll diejenige Aufsichtsbehörde zuständig sein, bei der sich der Hauptsitz des Unternehmens befindet. Die Bürgerinnen und Bürger sollen daneben die Möglichkeit haben, ihre Datenschutzverletzungen bei der für sie zuständigen Aufsichtsbehörde zu rügen und ihre informationellen Selbstbestimmungsrechte dort geltend zu machen. Die Europäische Kommission plant auch, die Sanktionsmöglichkeiten der Aufsichtsbehörden erheblich zu stärken und effektiver auszugestalten. Weiter soll das Prinzip der Selbstkontrolle durch betriebliche Datenschutzbeauftragte europaweit eingeführt werden. Die Europäische Kommission plant neben einer Verpflichtung zur Folgenabschätzung im Datenschutz bei einem Informationstechnologie-Einsatz eine obligatorische Bestellung von betrieblichen Datenschutzbeauftragten bei Unternehmen, die die Größe eines kleinen oder mittelständischen Unternehmens überschreiten. Wir hoffen, dass die Datenschutzverordnung zusammen mit der neuen Datenschutzrichtlinie nicht das in Deutschland und damit auch das im Land Bremen aktuell geltende Datenschutzrecht verschlechtern, sondern eine Vereinheitlichung auf hohem Datenschutzniveau stattfinden wird.

20. Die Entschließungen der Datenschutzkonferenzen im Jahr 2011

20.1 Beschäftigtendatenschutz stärken statt abbauen

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. und 17. März 2011)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt die Notwendigkeit, durch umfassende allgemein gültige Regelungen für den Datenschutz am Arbeitsplatz mehr Rechtssicherheit zu erreichen und bestehende Schutzlücken zu schließen. Dieser Ansatz erfordert klare gesetzliche Begrenzungen der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten. Die Bundesregierung und die Bundestagsfraktionen der Sozialdemokratischen Partei Deutschlands (SPD) und von Bündnis 90/Die Grünen haben hierzu Gesetzentwürfe vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Deutschen Bundestag, bei den Beratungen über Regelungen des Beschäftigtendatenschutzes insbesondere folgende notwendige Anforderungen sicherzustellen:

— Im Bewerbungsverfahren und im Beschäftigungsverhältnis

  — ist die Erforderlichkeit von Eignungstests und medizinischen Untersuchungen vor der Durchführung der jeweiligen Maßnahme zu dokumentieren,

  — sind Datenerhebungen nur zulässig, wenn und soweit diese Daten wegen der Art und der Ausübung der Tätigkeit oder der Bedingung ihrer Ausübung unabdingbar sind und entscheidende berufliche Anforderungen oder Hindernisse darstellen,

  — sind Eignungstests ausschließlich zulässig, wenn sie auf einer wissenschaftlichen Methode beruhen.

— Arbeitgeber müssen verpflichtet werden, Bewerberinnen und Bewerber so früh wie möglich umfassend über die Datenerhebung aus allgemein zugänglichen Quellen (zum Beispiel im Internet) und bei Dritten zu unterrichten.

— Zur Aufdeckung von Straftaten und ähnlich schwerwiegenden Pflichtverletzungen dürfen Beschäftigtendaten nur oberhalb normenklarer und verhältnismä-

ßiger Einschreitschwellen erhoben und verwendet werden. Arbeitgeber dürfen dabei – insbesondere verdeckte – Überwachungsmaßnahmen nur ergreifen, wenn zu dokumentierende Tatsachen vorliegen. Mit Blick auf rechtsstaatliche Anforderungen ist die Grenze zwischen eigenverantwortlichen Recherchen des Arbeitgebers und der den Strafverfolgungsbehörden vorbehaltenen Aufgaben eindeutig zu bestimmen. Aus präventiven Gründen ist eine verdeckte Datenerhebung unzulässig.

— Insbesondere bezüglich der Durchführung von Screening-Verfahren sind klare materielle Kriterien – zum Beispiel Prüfung der Verhältnismäßigkeit, Vorliegen von tatsächlichen Hinweisen auf Unregelmäßigkeiten – erforderlich. Zudem sollten Arbeitgeber verpflichtet sein, die näheren Umstände, die den Abgleich veranlassen, vorab zu dokumentieren.

— Die an verschiedenen Stellen im Gesetzentwurf der Bundesregierung vorgesehenen Regelungen zur Verhaltenskontrolle und Leistungskontrolle sind nach wie vor zu weitgehend. Der Gesetzgeber muss hier strenge Voraussetzungen vorgeben. Die Konferenz weist auf die gefestigte verfassungsrechtliche Rechtsprechung zum unzumutbaren Überwachungsdruck hin.

— Die Konferenz der Datenschutzbeauftragten fordert, die offene Videoüberwachung stärker zu begrenzen und insbesondere

  — zu verbieten, die zum Beispiel bei der Qualitätskontrolle anfallenden Daten zur Verhaltenskontrolle und Leistungskontrolle zu nutzen.

  — für Bereiche zu untersagen, die nicht nur „überwiegend“, sondern auch der privaten Nutzung dienen.

— Das Petitionsrecht darf nicht beschränkt werden. Beschäftigte müssen sich jederzeit an die zuständige Datenschutzaufsichtsbehörde wenden können, ohne deswegen benachteiligt oder gemaßregelt zu werden.

— In gesetzliche Regelungen zum Beschäftigtendatenschutz sind darüber hinaus Bestimmungen aufzunehmen

  — zur Personalaktenführung – einschließlich der automatisierten Personalaktenführung,

  — zur privaten Nutzung von Telekommunikationsdiensten,

  — zum Thema Whistleblowing,

  — zum Bereich der Videoüberwachung im öffentlich zugänglichen Bereich, bei denen Beschäftigtendaten mit anfallen,

  — zum Beweisverwertungsverbot bei unzulässiger Datenerhebung und Datenverwendung,

  — zum Konzerndatenschutz unter Berücksichtigung des internationalen Datenverkehrs.

20.2 Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. und 17. März 2011)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Oktober 2009 auf die Notwendigkeit einer datenschutzkonformen Gestaltung und Nutzung von Informationstechnik in Krankenhäusern hingewiesen.

Es besteht das dringende Bedürfnis, hierbei zu einem bundesweit und trägerübergreifend einheitlichen Verständnis der datenschutzrechtlichen Anforderungen zu gelangen, zumindest soweit dies Divergenzen in der Landeskrankenhausgesetzgebung erlauben. Zu diesem Zweck hat eine Unterarbeitsgruppe der Arbeitskreise „Gesundheit und Soziales“ und „Technik“ unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche eine Orientierungshilfe erarbeitet. Im Rahmen eines Kommentierungsverfahrens und bei Expertenanhörungen wurden Hersteller von Krankenhausinformationssystemen, Betreiber und Datenschutzbeauftragte von Krankenhäusern einbezogen. Die genannten Arbeitskreise haben die Orientierungshilfe verabschiedet.

Sie konkretisiert in ihrem ersten Teil die Anforderungen, die sich aus den datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben. In Teil 2 werden Maßnahmen zu deren technischer Umsetzung beschrieben. Für die Hersteller von Krankenhausinformationssystemen, die diese nutzenden Krankenhäuser und die internen Datenschutzbeauftragten von Krankenhäusern liegt damit erstmals ein Orientierungsrahmen für eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb entsprechender Verfahren vor. Für die Datenschutzbehörden wird das vorliegende Dokument als Maßstab bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontrolltätigkeit und Beratungstätigkeit dienen. Dabei ist zu berücksichtigen, dass ein Teil der am Markt angebotenen Lösungen nach den Erkenntnissen der Datenschutzbehörden in technischer Hinsicht gegenwärtig noch hinter den darin enthaltenen Anforderungen zurückbleibt. Es ist daher von der Notwendigkeit einer angemessenen Übergangsfrist für erforderliche Anpassungen durch die Hersteller auszugehen.

Stellen die Datenschutzbehörden im Zuge ihrer Kontrolltätigkeit Defizite im Vergleich zu den dargelegten Maßstäben fest, so werden sie auf die Krankenhäuser einwirken und sie dabei unterstützen, in einem geordneten Prozess unter Wahrung der Patientensicherheit Wege zur Behebung der Defizite zu finden und zu begehen. Die Deutsche Krankenhausgesellschaft und die jeweiligen Landeskrankenhausgesellschaften werden dabei einbezogen.

Die Erfahrungen der Prüftätigkeit sollen in eine regelmäßige Überarbeitung und Aktualisierung der Orientierungshilfe unter Berücksichtigung der technischen Weiterentwicklung einfließen. Die Arbeitskreise sind aufgefordert, diesen Revisionsprozess zu koordinieren und das Ergebnis spätestens im Frühjahr 2012 der Konferenz vorzulegen.

Die Konferenz nimmt die Orientierungshilfe zustimmend zur Kenntnis.

20.3 Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. und 17. März 2011)

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungszwecken, Behandlungszwecken und Dokumentationszwecken. Seit dem 1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Absatz 4 Strafgesetzbuch V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von Informationstechnologie-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe http://www.kbv.de/rechtsquellen/24631.html).

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 Strafgesetzbuch) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jahrgang 105, Heft 19 vom 9. Mai 2008) zu beachten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dabei insbesondere folgende Mindestanforderungen zu stellen:

1. Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.

2. Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.

3. Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.

4. Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.

5. Die Wartung der zum Netzzugang eingesetzten Hardware-Komponenten und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.

6. Zum Netzzugang sind zertifizierte Hardware-Komponenten und Software-Komponenten einzusetzen.

7. Grundstandards – wie beispielsweise die Revisionssicherheit – sind einzuhalten.

Für die verwendeten Verschlüsselungskomponenten und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

a) nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

b) — eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,

— mit der zum Zugang verwendeten Hardware und Software ausschließlich Zugang zu medizinischen Netzen besteht sowie

— die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden.

20.4 Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. und 17. März 2011)

Wollen Strafverfolgungsbehörden verschlüsselte Internetkommunikationsvorgänge (zum Beispiel Internettelefonie oder E-Mails) überwachen und aufzeichnen, muss regelmäßig auf dem Endgerät des Betroffenen eine Software angebracht werden, die die Daten aus dem laufenden Kommunikationsvorgang vor ihrer Verschlüsselung erfasst und an die Behörde weiterleitet (sogenannte Quellen-Telekommunikationsüberwachung). Die hierbei anzuwendende Technik entspricht der der Online-Durchsuchung, die grundsätzlich auch Zugriffe auf gespeicherte Inhalte ermöglicht.

Telekommunikationsüberwachungsmaßnahmen durch Zugriffe auf Endgeräte müssen sich auf Daten aus laufenden Telekommunikationsvorgängen beschränken. Dies ist durch technische Vorkehrungen und rechtliche Vorgaben sicherzustellen. Nur so wird der Rechtsprechung des Bundesverfassungsgerichts entsprochen.

Die Strafprozessordnung enthält keine Regelung, die diesen Anforderungen gerecht wird. Im grundrechtsrelevanten Bereich muss der Gesetzgeber alle wesentlichen Vorgaben selbst treffen. Es reicht nicht aus, wenn derartige Schutzvorkehrungen nur im Rahmen eines Gerichtsbeschlusses auf der Grundlage von §§ 100 a, 100 b Strafprozessordnung angeordnet werden. Vielmehr müssen die vom Bundesverfassungsgericht geforderten rechtlichen Vorgaben und technischen Vorkehrungen gesetzlich verankert sein.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, Rechtssicherheit – auch für die Strafverfolgungsbehörden – zu schaffen und die Zulässigkeit und die Voraussetzungen der Quellen-Telekommunikationsüberwachung unter strenger Beachtung der Vorgaben des Bundesverfassungsgerichts zu klären.

20.5 Keine Vorratsspeicherung und Rasterung von Flugpassagierdaten!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. und 17. März 2011)

Die EU-Kommission hat am 2. Februar 2011 einen neuen Entwurf für eine Richtlinie zur Nutzung von EU-Flugpassagierdaten zur Gefahrenabwehr und Strafverfolgung vorgestellt.

Zentraler Gegenstand des Entwurfs ist die systematische Erfassung der Daten aller Fluggäste, die EU-Außengrenzen überqueren. Diese Daten aus den Buchungssystemen der Fluggesellschaften sollen anlassunabhängig und verdachtsunabhängig an eine nationale Zentralstelle der Sicherheitsbehörden übermittelt und regelmäßig für fünf Jahre gespeichert werden. Ziel soll es sein, damit Personen ausfindig zu machen, die in Terrorismus oder schwere Kriminalität verwickelt sein könnten.

Auch der neue Entwurf bleibt konkrete Beweise dafür schuldig, dass die anlassfreie automatisierte Auswertung und Analyse von Flugpassagierdaten geeignet und erforderlich ist, um dieses Ziel zu fördern. Ein solches Zusammenspiel von Vorratsspeicherung und Rasterung von Passagierdaten ist weder mit der EU-Grundrechtecharta noch mit dem grundgesetzlich garantierten Recht auf informationelle Selbstbestimmung vereinbar. Dies gilt insbesondere im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts, das in seinem Urteil vom 2. März 2010 (1 BvR 256/08) zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten gemahnt hat: Zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört es, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Hierfür hat sich die Bundesrepublik auch auf europäischer und internationaler Ebene einzusetzen.

Ein solches System würde noch weiter reichende Eingriffe in die Bürgerrechte ermöglichen, wenn sogar Vorschläge zur Speicherung der Fluggastdaten bei Flügen innerhalb der Europäischen Union und von Daten der Bahnreisenden und Schiffsreisenden Eingang in diese Richtlinie finden würden.

Dieser Entwurf verdeutlicht erneut, dass ein schlüssiges Gesamtkonzept auf europäischer Ebene zur Datenverarbeitung im Bereich der inneren Sicherheit fehlt, welches die Grundrechte der Betroffenen hinreichend gewährleistet.

Die Konferenz fordert daher die Bundesregierung und den Bundesrat auf, sich dafür einzusetzen, dass der Vorschlag der EU-Kommission für eine Richtlinie über die Verwendung von Passagierdaten nicht realisiert wird.

20.6 Gravierende Defizite bei der Umsetzung des SWIFT-Abkommens – dringender Handlungsbedarf auf nationaler und europäischer Ebene

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. und 17. März 2011)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder missbilligt, dass – wie eine Prüfung der Gemeinsamen Kontrollinstanz von Europol ergeben hat[1]) – EU-Zahlungsdaten auf der Grundlage viel zu abstrakter Anfragen von US-Seite umfassend in die USA übermittelt wurden. Im Ergebnis wurden damit nicht einmal die im Abkommen festgelegten unzureichenden Datenschutzregeln beachtet. Das europäische Polizeiamt Europol hat jedem US-Ersuchen zugestimmt, obwohl aufgrund der Abstraktheit der schriftlichen Ersuchen mit nur mündlicher Begründung eine abkommenskonforme Erforderlichkeitsprüfung durch Europol nicht möglich war. Die angeforderten Daten wurden stets ohne Abstriche in die USA übermittelt. Diese Vorgehensweise ist mit dem SWIFT-Abkommen und der Europol darin zugewiesenen datenschutzrechtlichen Wächterfunktion nicht vereinbar.

Nach dem SWIFT-Abkommen muss Europol im Interesse der EU-Bürgerinnen und EU-Bürger gewährleisten, dass die Beschränkungen und Verfahrensvorgaben des Abkommens strikt beachtet werden. Europol ist demnach verpflichtet, alle US-Ersuchen auf die Beachtung dieser Beschränkungen und damit auf die Erforderlichkeit der Datenübermittlung zu überprüfen. Ohne die Zustimmung von Europol darf SWIFT keine EU-Zahlungsdaten an die USA übermitteln.

---

[1]) Der von der Gemeinsamen Kontrollinstanz von Europol vor wenigen Tagen veröffentlichte öffentliche Teil des Kontrollberichts zur Umsetzung des SWIFT-Abkommens ist auf der Homepage der GKI (http://europoljsb.consilium.europa.eu/about.aspx) abrufbar.

Die jetzt festgestellten Mängel bestätigen die bereits im Vorfeld des Abkommens von der Konferenz geäußerte Befürchtung, dass Europol seine Kontrollaufgabe bei SWIFT nicht angemessen wahrnimmt. Offenkundig werden die Voraussetzungen, unter denen das Europäische Parlament dem SWIFT-Abkommen zugestimmt hat, nicht eingehalten. Inakzeptabel ist auch, dass die festgestellten Details von Europol pauschal als geheim klassifiziert wurden und dem Europäischen Parlament nicht mitgeteilt werden sollen. Auch die Öffentlichkeit hat ein Recht darauf zu erfahren, in welchem Umfang Daten aufgrund des Abkommens in die USA übermittelt wurden.

Die Konferenz fordert die politisch Verantwortlichen auf europäischer und nationaler Ebene auf, die Mängel umgehend zu beseitigen. Das Abkommen und seine Umsetzungspraxis gehören dringend auf den Prüfstand. Ein transparentes Verfahren und die Beteiligung der Öffentlichkeit sind unabdingbar. Die gravierenden Mängel erfordern zudem einen sofortigen Stopp der Entwicklung eines vergleichbaren EU-Systems.

20.7 Funkzellenabfrage muss eingeschränkt werden!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juli 2011)

Die Strafverfolgungsbehörden in Dresden haben mit einer sogenannten Funkzellenabfrage anlässlich von Versammlungen und dagegen gerichteter Demonstrationen am 19. Februar 2011 Hunderttausende von Verkehrsdaten von Mobilfunkverbindungen erhoben, darunter die Rufnummern von Anrufern und Angerufenen, die Uhrzeit sowie Angaben zur Funkzelle, in der eine Mobilfunkaktivität stattfand. Dadurch sind zehntausende Versammlungsteilnehmerinnen und Versammlungsteilnehmer, darunter Abgeordnete von Landtagen und des Deutschen Bundestages, Rechtsanwältinnen und Rechtsanwälte, sowie Journalistinnen und Journalisten in Ausübung ihrer Tätigkeit, aber auch Anwohnerinnen und Anwohner der dicht besiedelten Dresdener Innenstadt, in ihrer Bewegung und ihrem Kommunikationsverhalten erfasst worden. Dieser Vorfall verdeutlicht die Schwäche der gesetzlichen Regelung.

Rechtsgrundlage der nichtindividualisierten Funkzellenabfrage ist bisher § 100 g Absatz 2 Satz 2 Strafprozessordnung (StPO), wonach im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation ausreichend sein soll, um Verkehrsdaten bei den Telekommunikationsdiensteanbietern erheben zu dürfen. Diese Aussage wird mit einer allgemeinen Subsidiaritätsklausel verknüpft. Diese 2001 in die Strafprozessordnung eingefügte Regelung ist unzureichend, da sie weder hinreichend bestimmt ist noch den heutigen technischen Gegebenheiten entspricht. Aktuelle Geräte erzeugen durch ihren Datenverkehr ohne aktives Zutun des Besitzers eine Vielzahl von Verkehrsdaten, die später in einer Funkzellenabfrage erhoben werden können.

Die Funkzellenabfrage ist ein verdeckter Eingriff in das Fernmeldegeheimnis (Artikel 10 Grundgesetz). Sie richtet sich unterschiedslos gegen alle in einer Funkzelle anwesenden Mobilfunkgerätebesitzer, nicht nur – wie etwa eine Telekommunikationsüberwachung nach § 100 a StPO – gegen bestimmte einzelne Tatverdächtige. Sie offenbart Art und Umstände der Kommunikation von unter Umständen Zehntausenden von Menschen, die selbst keinen Anlass für einen staatlichen Eingriff gegeben haben. Sie schafft damit des Weiteren die Möglichkeit, diese Personen rechtswidrig wegen Nicht-Anlasstaten, etwa Verstößen gegen das Versammlungsgesetz, zu verfolgen. Sie ist bezogen auf einzelne Personen ein Instrument der Verdachtsgenerierung. Die Strafprozessordnung regelt nicht näher, wie die Behörden mit den erhobenen Daten umzugehen haben, insbesondere nicht, über welche Zeiträume, zu welchen Personen und in welchen anderen Zusammenhängen die erhobenen Daten polizeilich weiter verwendet werden dürfen.

Das Bundesverfassungsgericht hat stets betont, dass die Erhebung von Verkehrsdaten erhebliche Rückschlüsse auf das Kommunikationsverhalten zulässt. Verkehrsdaten können das soziale Netz des Betroffenen widerspiegeln; allein aus ihnen kann die Verbindung zu Parteien, Gewerkschaften oder Bürgerinitiativen deutlich werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Bundesgesetzgeber auf, den Anwendungsbereich für eine nichtindividua-

lisierte Funkzellenabfrage einzuschränken, dem Grundsatz der Verhältnismäßigkeit zu stärkerer Beachtung in der Praxis zu verhelfen, das Erforderlichkeitsprinzip zu stärken (etwa durch die Pflicht zur unverzüglichen Reduzierung der erhobenen Daten auf das zur Strafverfolgung oder gerichtlichen Auseinandersetzung Erforderliche) sowie die Löschungsvorschrift des § 101 Absatz 8 StPO zu präzisieren.

20.8 Antiterrorgesetze zehn Jahre nach 9/11 – Überwachung ohne Überblick

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. und 29. September 2011)

In der Folge der Anschläge vom 11. September 2001 wurden der Polizei, den Strafverfolgungsbehörden und den Nachrichtendiensten zahlreiche neue Befugnisse eingeräumt, die sich durch eine große Streubreite auszeichnen und in die Grundrechte zahlreicher Bürgerinnen und Bürger eingreifen. Zunehmend werden Menschen erfasst, die nicht im Verdacht stehen, eine Straftat begangen zu haben oder von denen keine konkrete Gefahr ausgeht. Unbescholtene geraten so verstärkt in das Visier der Behörden und müssen zum Teil weitergehende Maßnahmen erdulden. Wer sich im Umfeld von Verdächtigen bewegt, kann bereits erfasst sein, ohne von einem Terrorhintergrund oder Verdacht zu wissen oder in entsprechende Aktivitäten einbezogen zu sein.

Zunehmend werden Daten, zum Beispiel über Flugpassagiere und Finanztransaktionen, in das Ausland übermittelt, ohne dass hinreichend geklärt ist, was mit diesen Daten anschließend geschieht (vergleiche dazu Entschließung der 67. Konferenz vom 25. und 26. März 2004 „Übermittlung von Flugpassagierdaten an die US-Behörden“; Entschließung der 78. Konferenz vom 8. und 9. Oktober 2009 „Kein Ausverkauf von europäischen Finanzdaten an die USA!“).

Das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 2. März 2010 (1 BvR 256/08) klargestellt: Es gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Die Verfassung fordert vielmehr ein austariertes System, bei dem jeder Eingriff in die Freiheitsrechte einer strikten Prüfung seiner Verhältnismäßigkeit standhält.

Von einem austarierten System der Eingriffsbefugnisse kann schon deshalb keine Rede sein, weil die Wechselwirkungen zwischen den verschiedenen Eingriffsinstrumentarien nie systematisch untersucht worden sind. Bundesregierung und Gesetzgeber haben bislang keine empirisch fundierten Aussagen vorgelegt, zu welchem Überwachungs-Gesamtergebnis die verschiedenen Befugnisse in ihrem Zusammenwirken führen. Die bislang nur in einem Eckpunktepapier angekündigte Regierungskommission zur Überprüfung der Sicherheitsgesetze ersetzt die erforderliche unabhängige wissenschaftliche Evaluation nicht.

Viele zunächst unter Zeitdruck erlassene Antiterrorgesetze waren befristet worden, um sie durch eine unabhängige Evaluation auf den Prüfstand stellen zu können. Eine derartige umfassende, unabhängige Evaluation hat jedoch nicht stattgefunden. Dies hat die Bundesregierung nicht davon abgehalten, gleichwohl einen Entwurf für die Verlängerung und Erweiterung eines der Antiterrorpakete in den Gesetzgebungsprozess einzubringen (Bundestags-Drucksache 17/6925).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher erneut, die Auswirkungen der bestehenden Sicherheitsgesetze – gerade in ihrem Zusammenwirken – durch eine unabhängige wissenschaftliche Evaluierung (so bereits die Entschließung der 79. Konferenz vom 17. und 18. März 2010 „Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich“) zu untersuchen. Die Wirksamkeit der Regelungen, ihre Erforderlichkeit für den gesetzgeberischen Zweck und ihre Angemessenheit, insbesondere im Hinblick auf die Bedrohungslage sowie die Auswirkungen für die Betroffenen müssen vor einer weiteren Befristung endlich kritisch überprüft werden.

20.9 Datenschutz als Bildungsaufgabe

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. und 29. September 2011)

Ein großer Teil der wirtschaftlichen, gesellschaftlichen und persönlichen Aktivitäten findet mittlerweile im Internet statt. Millionen von Bürgerinnen und Bürgern nutzen seine Möglichkeiten und gehen dabei auch besondere Risiken ein, ohne

dass ihnen dies immer bewusst wäre. Dies gilt insbesondere für Kinder und Jugendliche, aber auch erwachsene Internetnutzerinnen und Internetnutzer werden von der digitalen Welt zunehmend überfordert.

Vielen sind die Grundlagen, Funktionsbedingungen und wirtschaftlichen Spielregeln des Internet nicht oder nur zum Teil bekannt. Die meisten Internetnutzerinnen und Internetnutzer haben außerdem den Überblick darüber verloren, wer wann und zu welchem Zweck welche Daten von ihnen speichert, sie mit anderen Datensätzen verknüpft und gegebenenfalls auch an Dritte weitergibt. Wer aber nicht weiß, was mit seinen Daten geschieht oder geschehen kann, kann auch das informationelle Selbstbestimmungsrecht nicht effektiv ausüben.

Um dieser Entwicklung entgegenzuwirken, muss der Datenschutz auch als Bildungsaufgabe verstanden und praktiziert werden. Es genügt nicht, allein auf rechtliche Regelungen sowie auf datenschutzfreundliche technische Voreinstellungen und Anwendungen zu setzen. Die digitale Aufklärung ist unverzichtbar als Teil einer Datenschutzkultur des 21. Jahrhunderts. Sie beinhaltet zum einen die Vermittlung von Wissen und zum anderen die Entwicklung eines wachen, wertebezogenen Datenschutzbewusstseins.

So wie Bildung eine gesamtgesellschaftliche Aufgabe ist, so ist auch die Bildung im Hinblick auf die Datenschutzfragen unserer Zeit eine Aufgabe, die nicht nur dem Staat, sondern ebenso der Wirtschaft und der Zivilgesellschaft wie auch den Eltern im Verhältnis zu ihren Kindern obliegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt deshalb und unterstützt vielfältige Überlegungen und Aktivitäten, die sich stärker als bisher um eine größere Datenschutzkompetenz der Internetnutzenden bemühen.

Die Datenschutzkonferenz hält die bisherigen Bemühungen allerdings noch nicht für ausreichend. Will man die Internetnutzerinnen und Internetnutzer dazu befähigen, Vorteile und Gefahren von Internetangeboten abzuwägen und selbstverantwortlich zu entscheiden, in welchem Umfange sie am digitalen Leben teilhaben wollen, sind weitergehende und nachhaltige Anstrengungen notwendig. Vor allem ist sicherzustellen, dass

1. dabei viel intensiver als bisher die Möglichkeiten des Selbstdatenschutzes, der verantwortungsvolle Umgang mit den Daten anderer und die individuellen und gesellschaftlichen Auswirkungen einer leichtfertigen Nutzung des Internets thematisiert werden;
2. sich die schulischen und außerschulischen Programme und Projekte zur Förderung von Medienkompetenz nicht auf Fragen des Jugendmedienschutzes und des Urheberrechts beschränken, sondern den Datenschutz als wesentlichen Bestandteil mit einbeziehen;
3. Medienkompetenz und Datenschutzkompetenz entweder in einem eigenständigen Schulfach oder in einem Fächerspektrum mit Leitfächern verpflichtend zu verankern ist;
4. die Vermittlung von Datenschutz als integraler Bestandteil von Medienkompetenz ausdrücklich in den Bildungsstandards und Lehrplänen verankert wird und dass die entsprechenden Anforderungen bewertungsrelevant beziehungsweise prüfungsrelevant ausgestaltet werden und
5. Medienkompetenz und Datenschutzkompetenz und insbesondere die digitale Aufklärung zum verbindlichen Gegenstand der Lehrerausbildung gemacht werden.

Digitale Aufklärung und Erziehung zum Datenschutz bestimmen letztlich auch über den Stellenwert, den Privatsphäre und Persönlichkeitsrecht und damit Menschenwürde und Demokratie künftig in der internetgeprägten Gesellschaft insgesamt haben werden.

20.10 Datenschutzkonforme Gestaltung und Nutzung von Cloud Computing

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. und 29. September 2011)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert Cloud-Anbieter auf, ihre Dienstleistungen datenschutzkonform zu gestalten. Cloud-Anwender hingegen dürfen Cloud-Services nur dann in Anspruch nehmen, wenn

sie in der Lage sind, ihre Pflichten als verantwortliche Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutzanforderungen und Informationssicherheitsanforderungen geprüft haben.

Dies betrifft neben den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten insbesondere die in diesem Umfeld schwierig umzusetzenden Anforderungen an Kontrollierbarkeit, Transparenz und Beeinflussbarkeit der Datenverarbeitung. Cloud Computing darf nicht dazu führen, dass Daten verarbeitende Stellen, allen voran ihre Leitung, nicht mehr in der Lage sind, die Verantwortung für die eigene Datenverarbeitung zu tragen.

Zu verlangen sind also mindestens

— offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender einerseits entscheiden können, ob Cloud Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können;

— transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud-gestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und zur Interoperabilität;

— die Umsetzung der abgestimmten Sicherheitsmaßnahmen und Datenschutzmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender und

— aktuelle und aussagekräftige Nachweise (beispielsweise Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder bieten ihre Unterstützung bei der Entwicklung und bei der Nutzung von Cloud Computing-Diensten an. Details zur datenschutzgerechten Ausgestaltung dieser Dienste sind einer Orientierungshilfe[2]) der Arbeitskreise „Technik“ und „Medien“ zu entnehmen, die die Datenschutzkonferenz zustimmend zur Kenntnis genommen hat.

20.11 Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. und 29. September 2011)

Viele Betreiber und Anwender stellen in diesen Monaten ihre Netzwerktechnik auf das Internet-Protokoll Version 6 (IPv6) um. Grundsätzlich darf es mit einer Migration von IPv4 zu IPv6 nicht zu einer Verschlechterung der technischen Rahmenbedingungen zur Ausgestaltung von Privacy kommen. Neuen Herausforderungen muss mit wirksamen Konzepten begegnet werden.

IPv6 stellt eine nahezu unbegrenzte Anzahl von statischen IP-Adressen zur Verfügung, die eine dynamische Vergabe von IP-Adressen, wie sie zur Zeit bei Endkunden gängig ist, aus technischer Sicht nicht mehr erforderlich macht. Aber durch die Vergabe statischer Adressen erhöht sich das Risiko, dass Internetnutzende identifiziert und ihre Aktivitäten auf einfache Weise webseitenübergreifend zu individuellen Profilen zusammen geführt werden können. Sowohl der von den Internet-Providern bereitgestellte Adressanteil (Präfix) als auch gerätespezifische Anteile in den IPv6-Adressen machen eine dauerhafte Identifizierung möglich. Die Zuordnung einer IP-Adresse zu einer bestimmten Person bedarf nicht zwingend einer Beteiligung des Zugangsanbieters. Mit Hilfe von Zusatzinformationen, die dem Betreiber eines Internet-Angebots vorliegen oder ihm offenstehen, beispielsweise Identifikationskonten von Online-Shops oder Sozialen Netzen, ist eine eindeutige Zuordnung von Nutzern möglich. Die vereinfachten Möglichkeiten zur Profilbildung und Zusammenführung von Profilen erhöhen zudem das Risiko und verstärken die Auswirkungen krimineller Handlungen. Mit Blick darauf, dass sich ein Identifikationsrisiko aus beiden Teilen der neuen Adressen ergeben kann, sind Maßnahmen in unterschiedlichen Bereichen erforderlich.

———

[2]) http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

Die Datenschutzbeauftragten des Bundes und der Länder fordern, bei der Umstellung auf IPv6 Datenschutz und IT-Sicherheit zu gewährleisten. Anbieter von Internetzugängen und Diensten sowie Hersteller von Hardware-Lösungen und Software-Lösungen sollten ihre Produkte datenschutzgerecht gestalten *(privacy by design)* und dementsprechende Voreinstellungen wählen *(privacy by default)*. Internetnutzenden sollten bei der Beschaffung von Hardware und Software sowie beim Abschluss von Verträgen auf diese Aspekte besonders achten.

— Access Provider sollten Kundinnen und Kunden statische und dynamische Adressen ohne Aufpreis zuweisen. Auf Kundenwunsch sollten statische Adressen gewechselt werden können.

— Kundinnen und Kunden sollten mit nutzerfreundlichen Bedienelementen bei der Auswahl der Adressen für jeden von ihnen genutzten Dienst unterstützt werden.

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

— Die Hardwarehersteller und Softwarehersteller sollten Lösungen für dezentrale Kommunikationsdienste (peer to peer) in Kundensystemen entwickeln, die den Verzicht auf zentrale Plattformen und Portale ermöglichen. Sie sollten interessierten Dritten die Entwicklung solcher Dienste gestatten.

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

— Zugangsanbieter und Betreiber von Internetangeboten sollten nicht protokollierende Proxy-Server einsetzen und die Voraussetzungen schaffen, dass ein Internetzugang oder die Nutzung von im Internet bereitgestellten Inhalten in anonymer Form möglich ist (Anonymisierungsdienste).

— Hersteller und Anbieter von Betriebssystemen und vorkonfigurierten Geräten (wie PCs, Smartphones und Routern) sollten ihre Anstrengungen bei der Pflege und Weiterentwicklung ihrer Produkte intensivieren und regelmäßig Fehler bereinigte Versionen ihrer IPv6-fähigen Software anbieten.

— Angesichts häufig mangelnder Reife von IPv6-fähigen Produkten ist Anwendern vom Einsatz von IPv6 innerhalb von lokalen Netzen noch abzuraten, wenn dort sensible personenbezogene Daten verarbeitet werden sollen und funktionsfähige Filtereinrichtungen weder zentral noch auf den einzelnen Rechnern im LAN vorhanden und aktiviert sind.

— Eigentümerinnen und Eigentümer von IP-Adressen dürfen nur auf Wunsch in das weltweite, stark zentralisierte „Internet-Telefonbuch" *whois* aufgenommen werden. Die Bundesregierung wird aufgefordert, sich für eine datenschutzfreundliche Gestaltung des whois-Dienstes einzusetzen, dahingehend, dass die Internet-Verwaltung ICANN den whois-Dienst künftig als verteilte Datenbank gestaltet, so dass die Daten der Eigentümerinnen und Eigentümer jeweils durch lokale Dienstleister oder Selbstverwaltungsgremien gespeichert, gepflegt und von ihnen nach Maßgabe des lokalen Rechts an Dritte übermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder werden die Einführung von IPv6 wachsam beobachten und bieten allen Akteuren ihre Unterstützung an.

20.12 Datenschutz bei sozialen Netzwerken jetzt verwirklichen!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. und 29. September 2011)

Anlässlich der aktuellen Diskussionen um den Datenschutz bei sozialen Netzwerken, wie beispielsweise facebook, stellt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder klar, dass sich die Anbieter solcher Plattformen, die auf den europäischen Markt zielen, auch dann an europäische Datenschutzstandards halten müssen, wenn sie ihren Sitz außerhalb Europas haben.

Die Konferenz stellt insbesondere fest, dass die direkte Einbindung von Social-Plugins beispielsweise von facebook, Google+, Twitter und anderen Plattformbe-

treibern in die Webseiten deutscher Anbieter ohne hinreichende Information der Internet-Nutzenden und ohne Einräumung eines Wahlrechtes nicht mit deutschen und europäischen Datenschutzstandards in Einklang steht. Die aktuelle von Social-Plugin-Anbietern vorgesehene Funktionsweise ist unzulässig, wenn bereits durch den Besuch einer Webseite und auch ohne Klick auf beispielsweise den „Gefällt-mir"-Knopf eine Übermittlung von Nutzendendaten in die USA ausgelöst wird, auch wenn die Nutzenden gar nicht bei der entsprechenden Plattform registriert sind.

Die Social-Plugins sind nur ein Beispiel dafür, wie unzureichend einige große Betreiber sozialer Plattformen den Datenschutz handhaben. So verwendet facebook mittlerweile Gesichtserkennungs-Technik, um Bilder im Internet bestimmten Personen zuzuordnen; Betroffene können sich dem nur mit erheblichem Aufwand entziehen. Sowohl facebook als auch Google+ verlangen, dass die Nutzenden sich identifizieren, obwohl nach deutschem Recht aus guten Gründen die Möglichkeit zumindest einer pseudonymen Nutzung solcher Dienste eröffnet werden muss.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher alle öffentlichen Stellen auf, von der Nutzung von Social-Plugins abzusehen, die den geltenden Standards nicht genügen. Es kann nicht sein, dass die Bürgerinnen und Bürger, die sich auf den Seiten öffentlicher Stellen informieren wollen, mit ihren Daten dafür bezahlen. Unbeschadet der rechtlichen Verantwortung sollten die öffentlichen Stellen auf solchen Plattformen keine Profilseiten oder Fanpages einrichten.

Die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bereits 2008 und zuletzt 2010 in Beschlüssen Anforderungen an die datenschutzkonforme Gestaltung sozialer Netzwerke formuliert. Die Konferenz der Datenschutzbeauftragten fordert die Anbieter sozialer Netzwerke auf, diese Beschlüsse umzusetzen, soweit dies noch nicht geschehen ist. In diesem Zusammenhang unterstützen die Datenschutzbeauftragten Bestrebungen zur Entwicklung von technischen Lösungen zur datenschutzkonformen Gestaltung von Webangeboten.

Bedauerlicherweise hat die Bundesregierung ihrer schon im letzten Jahr gemachten Ankündigung, gesetzgeberische Maßnahmen gegen die Profilbildung im Internet vorzuschlagen, keine Taten folgen lassen. Der bloße Verweis darauf, dass die Diensteanbieter Selbstverpflichtungen eingehen sollten, wird dem akuten Schutzbedarf der immer zahlreicher werdenden Nutzerinnen und Nutzer nicht gerecht. Die Konferenz der Datenschutzbeauftragten unterstützt den Gesetzentwurf des Bundesrates zur Änderung des Telemediengesetzes (Bundestags-Drucksache 17/6765) als einen Schritt in die richtige Richtung.

20.13 Vorbeugender Grundrechtsschutz ist Aufgabe der Datenschutzbeauftragten!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. und 29. September 2011)

Der Sächsische Datenschutzbeauftragte hat mit einem Bericht zu den nicht individualisierten Funkzellenabfragen und anderen Maßnahmen der Telekommunikationsüberwachung im Februar 2011 durch die Polizei und die Staatsanwaltschaft Dresden Stellung genommen (Landtags-Drucksache 5/6787). In nicht nachvollziehbarer Weise ist die Kompetenz des Sächsischen Datenschutzbeauftragten zur Kontrolle von Verfahrensweisen von Polizei und Staatsanwaltschaften im Vorfeld einer beziehungsweise nach einer richterlichen Anordnung in Frage gestellt worden.

Die Konferenz ist der Auffassung, dass derartige Äußerungen von der gebotenen inhaltlichen Aufarbeitung der Dresdener Funkzellenabfragen ablenken. Die gesetzliche Befugnis des Sächsischen Datenschutzbeauftragten zur Kontrolle aller polizeilichen und staatsanwaltschaftlichen Maßnahmen der Datenverarbeitung steht außer Frage. Es ist auch im Bereich der Strafverfolgung eine verfassungsrechtlich begründete Kernaufgabe der unabhängigen Datenschutzbeauftragten, einen vorgezogenen Rechtsschutz dort zu gewährleisten, wo Einzelne aufgrund der verdeckten Datenverarbeitung des Staates nicht oder nicht ausreichend früh anderweitigen Rechtsschutz erlangen kann. Der Sächsische Datenschutzbeauftragte hat die polizeiliche Anregung bzw. staatsanwaltschaftliche Beantragung der konkreten Funkzellenabfragen als unverhältnismäßig und die besonderen Rechte von Abgeordneten, Verteidigerinnen und Verteidigern nicht wahrend beanstandet. Es kann dahinstehen, ob die funktional als Ausübung vollziehender Gewalt (vergleiche BVerfGE 107, 395, 406) zu qualifizierende richterliche Anordnung solcher Maßnahmen von Landesdatenschutzbeauftragten kontrolliert werden kann, da die jeweiligen richterlichen Anordnungen in den konkreten Fällen nicht beanstandet wurden.

20.14 Anonymes elektronisches Bezahlen muss möglich bleiben!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. und 29. September 2011)

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Bundesgesetzgeber auf, bei der Bekämpfung von Geldwäsche auf umfassende und generelle Identifizierungspflichten beim Erwerb von elektronischem Geld zu verzichten. Ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (Bundestags-Drucksache 17/6804) sieht vor, über bereits bestehende – allerdings nicht umgesetzte – gesetzliche Verpflichtungen hinaus umfangreiche Daten über sämtliche Erwerber elektronischen Geldes zu registrieren. Der anonyme Erwerb von E-Geld würde damit generell abgeschafft.

Dies ist besonders kritisch, da umfangreiche Kundinnendaten und Kundendaten unabhängig vom Wert des E-Geldes erhoben werden müssen. Beispielsweise ist eine Tankstelle bereits beim Verkauf einer E-Geld Karte im Wert von fünf Euro verpflichtet, den Namen, das Geburtsdatum und die Anschrift der Kundinnen und Kunden zu erheben und für mindestens fünf Jahre aufzubewahren.

Eine generelle Identifizierungspflicht würde außerdem dazu führen, dass anonymes Einkaufen und Bezahlen im Internet selbst bei Bagatellbeträgen praktisch ausgeschlossen werden. Anonyme Bezahlsysteme im Internet bieten ihren Nutzern jedoch Möglichkeiten, die Risiken eines Missbrauchs ihrer Finanzdaten beispielsweise durch Hackerangriffe zu minimieren. Sie sind zugleich ein wichtiger Baustein, um die Möglichkeit zum anonymen Medienkonsum zu erhalten, da Online-Medien zunehmend gegen Bezahlung angeboten werden. Auf jeden Fall muss verhindert werden, dass personenbeziehbare Nutzungsdaten über jeden einzelnen Artikel in Onlinezeitungen oder einzelne Sendungen im Internet-TV schon immer dann entstehen, wenn eine Nutzung gebührenpflichtig ist.

Nach den vorgesehenen Regelungen würden noch mehr personenbezogene Daten unbescholtener Bürgerinnen und Bürger erfasst und ganz überwiegend anlasslos gespeichert. Dies steht in Widerspruch zur Rechtsprechung des Bundesverfassungsgerichts. In seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 2. März 2010 (1 BvR 256/08) hatte das Gericht gemahnt, dass Gesetze, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielen, mit der Verfassung unvereinbar sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die vorgesehene verdachtsunabhängige, undifferenzierte und schrankenlose Datenerfassung ab, die auch europarechtlich nicht geboten ist. Die dritte Geldwäscherichtlinie (2005/60/EG) erlaubt den Mitgliedstaaten, von Identifizierungspflichten abzusehen, wenn der Wert des erworbenen elektronischen Guthabens 150 Euro nicht übersteigt. Der Bundesgesetzgeber sollte durch Einführung eines entsprechenden Schwellenwerts diesem risikoorientierten Ansatz folgen.

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

21.1 Datenschutz-Kodex des BITKOM für Geodatendienste unzureichend – Gesetzgeber gefordert

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 8. April 2011)

Am 1. März 2011 hat der Branchenverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) einen Datenschutz-Kodex für Geodatendienste vorgelegt, der den schutzwürdigen Interessen der Eigentümer und Bewohner bei der Veröffentlichung der sie betreffenden Gebäudeansichten im Internet Rechnung tragen soll. Das Bundesministerium des Innern hatte der Internetwirtschaft in Aussicht gestellt, bei der Vorlage einer angemessenen und mit den Datenschutzbehörden des Bundes und der Länder abgestimmten Selbstverpflichtung auf gesetzliche Spezialregelungen für Internet-Geodatendienste wie Google Street View zu verzichten.

Der Düsseldorfer Kreis stellt fest, dass die Selbstregulierung der Internetwirtschaft mit dem vom BITKOM vorgelegten Datenschutz-Kodex nicht gelingt. Der Kodex

entspricht in wesentlichen Bereichen nicht den datenschutzrechtlichen Anforderungen und ist nicht mit den Datenschutzbehörden des Bundes und der Länder abgestimmt.

Der Kodex sieht zwar ein Widerspruchsrecht gegen die Veröffentlichung von Gebäudeansichten im Internet vor, ohne dass Gründe dargelegt werden müssen. Der Widerspruch ist jedoch erst nach der Veröffentlichung vorgesehen. Alle Gebäudeansichten sind deshalb zunächst im Internet verfügbar. Bereits mit der Veröffentlichung der Bilder wird aber das Recht auf informationelle Selbstbestimmung verletzt. Auch bei weiteren Regelungen weist der Datenschutz-Kodex datenschutzrechtliche Defizite auf: Viele Veröffentlichungen, die die Privatsphäre beeinträchtigen, werden vom Kodex nicht erfasst, so etwa Schrägaufnahmen aus der Luft. Hinzu kommt, dass der Datenschutz-Kodex nur für die Unternehmen bindend ist, die ihn unterzeichnet haben.

Deshalb ist jetzt der Gesetzgeber gefordert, das Recht auf informationelle Selbstbestimmung im Internet mit einer umfassenden Regelung zu schützen, die dem besonderen Gefährdungspotenzial für das Persönlichkeitsrecht im Internet Rechnung trägt. Hierzu zählt insbesondere ein gesetzlich verbrieftes Widerspruchsrecht gegen die Veröffentlichung, das es den Betroffenen ermöglicht, bereits vor der Veröffentlichung personenbezogener Daten im Internet Widerspruch einzulegen.

Ein solches Vorab-Widerspruchsrecht entspricht den Anforderungen, die der Düsseldorfer Kreis in seinem Beschluss vom 13. und 14. November 2008 nach Auslegung des geltenden Rechts konkretisiert hat. Besonders wichtig sind demnach die folgenden Punkte:

— Gesichter und Kfz-Kennzeichen sind unkenntlich zu machen.

— Eigentümer und Bewohner eines Hauses müssen die Möglichkeit erhalten, die Veröffentlichung der Gebäudefassade durch einen Widerspruch zu verhindern; die Widerspruchsmöglichkeit muss vor wie auch nach der Veröffentlichung bestehen.

— Die geplante Datenerhebung und der Hinweis auf die Widerspruchsmöglichkeit sind rechtzeitig bekannt zu geben.

21.2 Datenschutzgerechte Smartphone-Nutzung ermöglichen!

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich am 4. und 5. Mai 2011 in Düsseldorf)

Smartphones sind Mobiltelefone, die insbesondere im Zusammenhang mit der Nutzung des Internet über deutlich mehr Computerfunktionalitäten und Kommunikationsmöglichkeiten verfügen als herkömmliche Mobiltelefone. Smartphones werden für eine Vielzahl von Aktivitäten genutzt und sind damit in weitaus größerem Umfang als sonstige Geräte der Informationstechnik und Kommunikationstechnik „persönliche“ Geräte, die den Nutzer im Alltag permanent begleiten. Über das Telefonieren hinaus eröffnen auf den Geräten installierbare Programme („Apps“), Lokalisierungsfunktionen (GPS) und Bewegungssensoren eine breite Palette von Anwendungsbereichen. Die dabei anfallenden Daten lassen detaillierte Rückschlüsse auf Nutzungsgewohnheiten, Verhaltensweisen oder Aufenthaltsorte der Nutzer zu.

Im Gegensatz zu herkömmlichen PCs bieten Smartphones den Nutzern jedoch nur rudimentäre Möglichkeiten, die Preisgabe personenbezogener Daten zu kontrollieren oder zu vermeiden; gängige Funktionen des Selbstdatenschutzes können nicht genutzt werden. Häufig werden personenbezogene Daten ohne Wissen der Nutzer an die Anbieter von Diensten übermittelt. Mit einiger Berechtigung wird davon gesprochen, ein solches Gerät sei ein „Spion in der Hosentasche“. Vor diesem Hintergrund ist aus datenschutzrechtlicher Sicht insbesondere Folgendes zu fordern:

— Transparenz bezüglich der Preisgabe personenbezogener Daten:

In allen aktuellen Untersuchungen zeigt sich, dass in einer Vielzahl von Fällen durch die Geräte selbst mittels Betriebssystemen oder durch Anwendungen eindeutige Gerätekennungen, Standortdaten, E-Mail-Takte und Telefontakte, SIMKartennummer und weitere personenbezogene Daten ohne Unterrichtung der Nutzer an Gerätehersteller, Provider oder Anbieter von Analysediensten übermittelt werden. Die Nutzer müssen in die Lage versetzt werden, diese Übermittlungen nachzuvollziehen. Sie müssen auch über den jeweiligen Zweck der Datennutzungen unterrichtet werden.

— Steuerungsmöglichkeiten der Nutzer für die Preisgabe personenbezogener Daten:

Die Konzepte gängiger Smartphones sind oftmals darauf reduziert, dass, wenn überhaupt, lediglich während der Installation einer Anwendung der Nutzer pauschal einen Datenzugriff steuern kann. Auch erhalten zugelassene Anwendungen meist eine generelle Zugriffsmöglichkeit zum Beispiel auf Kontaktinformationen. Den Nutzern müssen Möglichkeiten an die Hand gegeben werden, mit denen aus der Nutzungssituation heraus gesteuert werden kann, ob und welche Daten einer Applikation zugänglich gemacht werden und an wen sie übermittelt werden.

— Einflussmöglichkeiten auf das Löschen von Spuren bei der Internet-Nutzung:

Im Gegensatz zu der für herkömmliche PCs bestehenden Situation fehlt es im Smartphonebereich weitgehend an Möglichkeiten, Datenspuren, die bei der Internet-Nutzung auf dem Gerät entstehen, zu vermeiden, zu reduzieren, mindestens jedoch, diese erkennbar zu machen und gegebenenfalls zu löschen. Solche Möglichkeiten müssen geschaffen und angeboten werden.

— Anonyme und pseudonyme Nutzungsmöglichkeiten:

Generell sollte die Möglichkeit geschaffen werden, Smartphones und die über sie vermittelten Dienste anonym oder pseudonym zu nutzen.

Die Anbieter entsprechender Geräte beziehungsweise Betriebssysteme und die jeweiligen Diensteanbieter müssen möglichst datenschutzfreundliche Funktionalitäten vorsehen und Schwachpunkte eliminieren. Der Grundsatz der Datensparsamkeit ist ernst zu nehmen und umzusetzen. Von besonderer Bedeutung ist die umfassende Information der Nutzer über die Erhebung und Verwendung ihrer Nutzungsdaten. Dies gilt sowohl für die grundlegenden Betriebssysteme einerseits wie für die darauf aufbauenden Funktionalitäten (Apps) andererseits. Diese Anforderungen lassen sich unter den Begriff „Privacy by Design“ fassen; auf den Inhalt und die Bedeutung dieses Punktes hat jüngst die Internationale Konferenz der Datenschutzbeauftragen hingewiesen (Resolution on Privacy by Design vom 29. Oktober 2010).

Der Aufgabe, den Selbstdatenschutz zu stärken, kommt im Bereich der Smartphone-Nutzung eine besondere Bedeutung zu. Die Datenschutzaufsichtsbehörden unterstützen alle entsprechenden Anstrengungen, insbesondere auch die der European Network and Information Security Agency (ENISA; vergleiche Empfehlungen der ENISA vom Dezember 2010 über Informationssicherheitsrisiken, Möglichkeiten und Empfehlungen für Nutzer von Smartphones; http://www.enisa.europa.eu/act/it/oar/smartphones-information-security-risksopportunities-and-recommendations-for-users/at_download/fullReport).

21.3 Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich am 4. und 5. Mai 2011 in Düsseldorf)

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

Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln. Die Aufsichtsbehörden im nichtöffentlichen Bereich fordern daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Es besteht das dringende Bedürfnis, hierbei zu einem bundesweit und trägerübergreifend einheitlichen Verständnis der datenschutzrechtlichen Anforderungen zu gelangen, zumindest soweit dies Divergenzen in der Landeskrankenhausgesetz-

gebung erlauben. Zu diesem Zweck wurde von den Datenschutzbeauftragten der Länder unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche eine Orientierungshilfe erarbeitet. Im Rahmen eines Kommentierungsverfahrens und bei Expertenanhörungen wurden Hersteller von Krankenhausinformationssystemen, Betreiber und Datenschutzbeauftragte von Krankenhäusern einbezogen.

Die Orientierungshilfe konkretisiert in ihrem ersten Teil die Anforderungen, die sich aus den datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben. In Teil 2 werden Maßnahmen zu deren technischer Umsetzung beschrieben. Für die Hersteller von Krankenhausinformationssystemen, die diese nutzenden Krankenhäuser und die internen Datenschutzbeauftragten von Krankenhäusern liegt damit erstmals ein Orientierungsrahmen für eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb entsprechender Verfahren vor.

Die Aufsichtsbehörden im nicht-öffentlichen Bereich werden sich an dem vorliegenden Dokument als Leitlinie bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit orientieren. Dabei ist zu berücksichtigen, dass ein Teil der am Markt angebotenen Lösungen nach den Erkenntnissen der Datenschutzbehörden in technischer Hinsicht gegenwärtig noch hinter den darin enthaltenen Anforderungen zurückbleibt. Es ist daher von der Notwendigkeit einer angemessenen Übergangsfrist für erforderliche Anpassungen durch die Hersteller auszugehen.

Stellen die Aufsichtsbehörden im Zuge ihrer Kontrolltätigkeit Defizite im Vergleich zu den dargelegten Maßstäben fest, so werden sie auf die Krankenhäuser einwirken und sie dabei unterstützen, in einem geordneten Prozess unter Wahrung der Patientensicherheit Wege zur Behebung der Defizite zu finden und zu begehen. Die Deutsche Krankenhausgesellschaft und die jeweiligen Landeskrankenhausgesellschaften werden dabei einbezogen.

Die Erfahrungen der Prüftätigkeit sollen in eine regelmäßige Überarbeitung und Aktualisierung der Orientierungshilfe unter Berücksichtigung der technischen Weiterentwicklung einfließen.

Die Aufsichtsbehörden nehmen die Orientierungshilfe zustimmend zur Kenntnis.

21.4 Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 4. und 5. Mai 2011 in Düsseldorf)

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungszwecken, Behandlungszwecken und Dokumentationszwecken. Seit dem 1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Absatz 4 Strafgesetzbuch V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe http://www.kbv.de/rechtsquellen/24631.html).

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 Strafgesetzbuch) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jahrgang 105, Heft 19 vom 9. Mai 2008) zu beachten.

An die Anbindung von Praxis-EDV-Systemen an medizinische Netze sind folgende Mindestanforderungen zu stellen:

1. Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.

2. Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.

3. Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.

4. Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.

5. Die Wartung der zum Netzzugang eingesetzten Hardware-Komponenten und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.

6. Zum Netzzugang sind zertifizierte Hardware-Komponenten und Software-Komponenten einzusetzen.

7. Grundstandards – wie beispielsweise die Revisionssicherheit – sind einzuhalten.

Für die verwendeten Verschlüsselungskomponenten und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

a) nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

b) — eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,

— mit der zum Zugang verwendeten Hardware und Software ausschließlich Zugang zu medizinischen Netzen besteht sowie

— die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden.

21.5 Beschäftigtenscreening bei AEO-Zertifizierung wirksam begrenzen

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich am 22. und 23. November 2011 in Düsseldorf)

Der Düsseldorfer Kreis hat sich bereits mehrfach mit dem Problem des Mitarbeiterscreenings befasst, zuletzt durch Beschluss vom 23. und 24. April 2009. Es gibt Anlass, die Problematik erneut aufzugreifen.

In den letzten Jahren ist insbesondere die Zollverwaltung im Rahmen der Bewilligung des zollrechtlichen Status eines „zugelassenen Wirtschaftsbeteiligten“ (AEO-Zertifizierungen) dazu übergegangen, von den Unternehmen umfangreiche Screenings von Mitarbeitern – und gegebenenfalls Daten Dritter – zu verlangen. Diese Screenings werden zum Teil in Abständen von wenigen Wochen ohne konkreten Anlass und undifferenziert durchgeführt. In diesem Geschäftsfeld betätigen sich bereits spezialisierte Dienstleister, die sich die bestehende Unsicherheit bei den Unternehmen zunutze machen. Dies ist auch der Grund, warum diese Screenings immer häufiger durchgeführt werden. Nach den praktischen Erfahrungen der Aufsichtsbehörden mangelt es an klaren Regelungen, wie mit den Ergebnissen von Datenscreenings umzugehen ist (Treffermanagement). Das Bundesministerium der Finanzen hat zwar am 14. Juni 2010 anlässlich dieser Praxis einschränkende Vorgaben erlassen, diese werden jedoch von den zuständigen Zollbehörden nicht einheitlich umgesetzt. Der Düsseldorfer Kreis hält in seinem vorgenannten Beschluss derartige Screenings nur aufgrund einer speziellen Rechtsgrundlage für zulässig. Eine solche Rechtsgrundlage fehlt.

Weder die geltenden EU-Antiterrorverordnungen noch andere Sanktionslisten erfüllen die Anforderungen an eine solche spezielle Rechtsgrundlage. Diese Verord-

nungen enthalten lediglich die allgemeine Handlungspflicht, den in den Anlagen genannten Personen und Institutionen keine rechtlichen Vorteile zu gewähren, verpflichten jedoch nicht zu Screenings von Mitarbeitern, Kunden oder Lieferanten.

Auch die Bundesregierung ist der Auffassung, dass die Terrorismusverordnungen keinen systematischen, anlassunabhängigen Abgleich von Mitarbeiterdateien mit den Sanktionslisten verlangen. Allenfalls nach Maßgabe von Sorgfaltspflichten und differenzierend nach verschiedenen Verkehrskreisen und Risikolagen seien solche Abgleiche zulässig. Es bleibe den Unternehmen überlassen, wie sie die Einhaltung der Terrorismusverordnungen sicherstellen (Bundestags-Drucksache 17/4136 vom 03.12.2010).

Vor diesem Hintergrund empfiehlt und fordert der Düsseldorfer Kreis:

— Unternehmen sollten Datenscreenings nicht pauschal und anlasslos durchführen. Da die Lohnzahlung nur unbar erfolgt, die Kreditinstitute nach § 25 c Kreditwesengesetz (KWG) ohnehin Abgleiche mit den Terrorlisten vornehmen, ist ein Datenabgleichverfahren innerhalb des Unternehmens mit Mitarbeiterdaten nicht geboten.

— Die Zollbehörden werden aufgefordert, die rechtsstaatlichen Vorgaben im Rahmen der AEO-Zertifizierung zu beachten. Eine einheitliche Praxis nach diesen Vorgaben gibt den Unternehmen Rechtssicherheit.

— Die Bundesregierung wird gebeten, die derzeitige AEO-Zertifizierungspraxis einer baldigen und umfassenden Evaluation zu unterziehen.

21.6 Anonymes und pseudonymes elektronisches Bezahlen von Internet-Angeboten ermöglichen!

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 22. bis 23. November 2011 in Düsseldorf)

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben zur Kenntnis genommen, dass zahlreiche Internet-Anbieter planen, ihre Geschäftsmodelle so umzustellen, dass ihre Angebote – insbesondere Informationsdienste und Medieninhalte – nicht mehr nur werbefinanziert, sondern auch gegen Bezahlung angeboten werden. Das darf nicht dazu führen, dass den Nutzern die Möglichkeit genommen wird, sich im Internet anonym zu bewegen und Inhalte zur Kenntnis zu nehmen, ohne dass sie sich identifizieren müssen.

Das Recht, sich möglichst anonym aus öffentlichen Quellen zu informieren, ist durch das Recht auf informationelle Selbstbestimmung und durch Artikel 5 Grundgesetz (Recht auf Informationsfreiheit) verfassungsrechtlich geschützt. Dementsprechend ist in § 13 Absatz 6 Telemediengesetz vorgeschrieben, dass die Möglichkeit bestehen muss, Telemedien anonym oder unter Pseudonym zu nutzen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren.

Diese Rechte sind in Gefahr, wenn Daten über die Nutzung einzelner Medienangebote entstehen. Wenn Inhalte gegen Bezahlung angeboten werden sollen, muss verhindert werden, dass personenbeziehbare Daten über jeden einzelnen Abruf von Beiträgen aus Online-Zeitungen oder einzelner Sendungen im Internet-TV entstehen.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich fordern die Anbieter von Telemedien auf, ihren gesetzlichen Verpflichtungen aus § 13 Absatz 6 des Telemediengesetzes bei der Einführung von kostenpflichtigen Inhalten nachzukommen. Es muss ein Bezahlungsverfahren angeboten werden, das „auf der ganzen Linie“ anonym oder mindestens pseudonym ausgestaltet ist. Eine Zahlung über pseudonyme Guthabenkarten würde die datenschutzrechtlichen Anforderungen erfüllen. Es reicht dagegen nicht aus, wenn sich zum Beispiel der Inhalteanbieter für die Abwicklung der Zahlverfahren eines Dritten bedient und dieser eine Identifizierung der Betroffenen verlangt.

Die Kreditwirtschaft hat es bisher versäumt, datenschutzgerechte Verfahren mit ausreichender Breitenwirkung anzubieten oder zu unterstützen. Die Aufsichtsbehörden fordern diese auf, zu überprüfen, inwieweit bereits im Umlauf befindliche elektronische Zahlungsmittel (wie zum Beispiel die Geldkarte) zu einem zumindest

pseudonymen Zahlungsmittel für Telemedien weiterentwickelt werden können. Dies könnte zum Beispiel durch die Ausgabe nicht personengebundener „White Cards“ erfolgen, die über Einzahlungsautomaten bei Banken und anderen Kreditinstituten anonym aufgeladen werden können.

Schließlich nehmen die Aufsichtsbehörden mit Sorge zur Kenntnis, dass ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (Bundestags-Drucksache 17/6804) die Gefahr birgt, dass das anonyme elektronische Bezahlen gesetzlich unterbunden wird. Die Intention des Telemediengesetzes, die pseudonyme beziehungsweise anonyme Nutzung von Telemedien zu ermöglichen, würde zunichte gemacht. Die Aufsichtsbehörden unterstützen die Forderung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28. und 29. September 2011 in München, die Möglichkeit zum elektronischen anonymen Bezahlen insbesondere für Kleinbeträge (sogenanntes Micropayment) zu erhalten[3]).

21.7 Datenschutz in sozialen Netzwerken

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich vom 8. Dezember 2011)

Der Düsseldorfer Kreis sieht die Bemühungen von Betreibern von sozialen Netzwerken als Schritt in die richtige Richtung an, durch Selbstverpflichtungen den Datenschutz von Betroffenen zu verbessern. Er unterstreicht, dass eine Anerkennung von Selbstverpflichtungen durch die Datenschutzaufsichtsbehörden gemäß § 38 a Bundesdatenschutzgesetz (BDSG) die Gewähr dafür bietet, dass die Anforderungen des geltenden Datenschutzrechts erfüllt werden und ein Datenschutzmehrwert entsteht.

Ungeachtet dieser allgemeinen Bemühungen um eine Verbesserung des Datenschutzes in sozialen Netzwerken müssen die Betreiber schon heute das Datenschutzrecht in Deutschland beachten. Für deutsche Betreiber ist dies unumstritten. Aber auch Anbieter, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, unterliegen hinsichtlich der Daten von Betroffenen in Deutschland gemäß § 1 Absatz 5 Satz 2 BDSG dem hiesigen Datenschutzrecht, soweit sie ihre Datenerhebungen durch Rückgriff auf Rechner von Nutzerinnen und Nutzern in Deutschland realisieren. Dies ist regelmäßig der Fall. Die Anwendung des BDSG kann in diesen Fällen nicht durch das schlichte Gründen einer rechtlich selbstständigen Niederlassung in einem anderen Staat des Europäischen Wirtschaftsraumes umgangen werden (§ 1 Absatz 5 Satz 1 BDSG). Nur wenn das soziale Netzwerk auch in der Verantwortung dieser europäischen Niederlassung betrieben wird, kann die Verarbeitung der Daten deutscher Nutzerinnen und Nutzer unter Umständen dem Datenschutzrecht eines anderen Staates im Europäischen Wirtschaftsraum unterliegen.

Betreiber von sozialen Netzwerken müssen insbesondere folgende Rechtmäßigkeitsanforderungen beachten, wenn sie in Deutschland aktiv sind:

— Es muss eine leicht zugängliche und verständliche Information darüber gegeben werden, welche Daten erhoben und für welche Zwecke verarbeitet werden. Denn nur eine größtmögliche Transparenz bei Abschluss des Vertrags über eine Mitgliedschaft beziehungsweise informierte Einwilligungen gewährleisten die Wahrung des Rechts auf informationelle Selbstbestimmung. Die Voreinstellungen des Netzwerkes müssen auf dem Einwilligungsprinzip beruhen, jedenfalls soweit nicht der Zweck der Mitgliedschaft eine Angabe von Daten zwingend voraussetzt. Eine Datenverarbeitung zunächst zu beginnen und nur eine Widerspruchsmöglichkeit in den Voreinstellungen zu ermöglichen, ist nicht gesetzmäßig.

— Es muss eine einfache Möglichkeit für Betroffene geben, ihre Ansprüche auf Auskunft, Berichtigung und Löschung von Daten geltend zu machen. Grundvoraussetzung hierfür ist die Angabe von entsprechenden Kontaktdaten an leicht auffindbarer Stelle, damit die Betroffenen wissen, wohin sie sich wenden können.

— Die Verwertung von Fotos für Zwecke der Gesichtserkennung und das Speichern und Verwenden von biometrischen Gesichtserkennungsmerkmalen sind

———

[3]) Vergleiche Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28. und 29. September 2011 in München: „Anonymes elektronisches Bezahlen muss möglich bleiben!“

ohne ausdrückliche und bestätigte Einwilligung der abgebildeten Person unzulässig.

— Das Telemediengesetz erfordert jedenfalls pseudonyme Nutzungsmöglichkeiten in sozialen Netzwerken. Es enthält im Hinblick auf Nutzungsdaten – soweit keine Einwilligung vorliegt – ein Verbot der personenbeziehbaren Profilbildung und die Verpflichtung, nach Beendigung der Mitgliedschaft sämtliche Daten zu löschen.

— Das direkte Einbinden von Social Plugins, beispielsweise von facebook, Google+ oder Twitter, in Websites deutscher Anbieter, wodurch eine Datenübertragung an den jeweiligen Anbieter des Social Plugins ausgelöst wird, ist ohne hinreichende Information der Internetnutzerinnen und Internetnutzer und ohne ihnen die Möglichkeit zu geben, die Datenübertragung zu unterbinden, unzulässig.

— Die großen Mengen an teils auch sehr sensiblen Daten, die in sozialen Netzwerken anfallen, sind durch geeignete technisch-organisatorische Maßnahmen zu schützen. Anbieter müssen nachweisen können, dass sie solche Maßnahmen getroffen haben.

— Daten von Minderjährigen sind besonders zu schützen. Datenschutzfreundlichen Standardeinstellungen kommt im Zusammenhang mit dem Minderjährigenschutz besondere Bedeutung zu. Informationen über die Verarbeitung von Daten müssen auf den Empfängerhorizont von Minderjährigen Rücksicht nehmen und also auch für diese leicht verständlich sein.

— Betreiber, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, müssen gemäß § 1 Absatz 5 Satz 3 BDSG einen Inlandsvertreter bestellen, der Ansprechperson für die Datenschutzaufsicht ist.

In Deutschland ansässige Unternehmen, die durch das Einbinden von Social Plugins eines Netzwerkes auf sich aufmerksam machen wollen oder sich mit Fanpages in einem Netzwerk präsentieren, haben eine eigene Verantwortung hinsichtlich der Daten von Nutzerinnen und Nutzern ihres Angebots. Es müssen zuvor Erklärungen eingeholt werden, die eine Verarbeitung von Daten ihrer Nutzerinnen und Nutzer durch den Betreiber des sozialen Netzwerkes rechtfertigen können. Die Erklärungen sind nur dann rechtswirksam, wenn verlässliche Informationen über die dem Netzwerkbetreiber zur Verfügung gestellten Daten und den Zweck der Erhebung der Daten durch den Netzwerkbetreiber gegeben werden können.

Anbieter deutscher Websites, die in der Regel keine Erkenntnisse über die Datenverarbeitungsvorgänge haben können, die beispielsweise durch Social Plugins ausgelöst werden, sind regelmäßig nicht in der Lage, die für eine informierte Zustimmung ihrer Nutzerinnen und Nutzer notwendige Transparenz zu schaffen. Sie laufen Gefahr, selbst Rechtsverstöße zu begehen, wenn der Anbieter eines sozialen Netzwerkes Daten ihrer Nutzerinnen und Nutzer mittels Social Plugin erhebt. Wenn sie die über ein Plugin mögliche Datenverarbeitung nicht überblicken, dürfen sie daher solche Plugins nicht ohne weiteres in das eigene Angebot einbinden.

22. Die Europäische und die Internationale Datenschutzkonferenz

Die Entschließung der Europäischen Datenschutzkonferenz im Jahr 2011 steht auf der Internetseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter

http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/EuDSK/EntschliessungEUDSK_deutsch.html?nn=409534

zur Verfügung.

Die Entschließung lautet:

— Notwendigkeit eines umfassenden Rahmens für den Datenschutz

Informationen zur Internationalen Datenschutzkonferenz sind unter

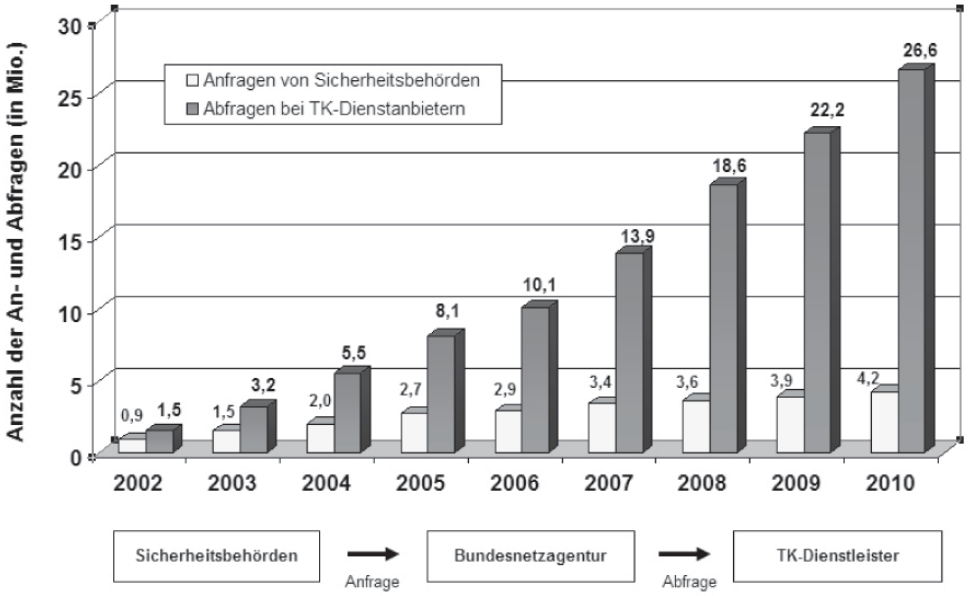
http://www.bfdi.bund.de/DE/EuropaUndInternationales/GremienOrganisation/Artikel/DieInternationaleDatenschutzkonferenz.html?nn=409534

zu finden.

23. Anhang

23.1 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 2002 bis 2010 dargestellt.



Quelle: Tätigkeitsbericht 2010/2011 der Bundesnetzagentur

23.2 Liste des verfügbaren Informationsmaterials

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

23.3 Index

Druck: Anker-Druck Bremen