BREMISCHE BÜRGERSCHAFT **Drucksache 18 / 1795**
Landtag 20. 03. 15
18. Wahlperiode

37. Jahresbericht der Landesbeauftragten für Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats meinen Bericht über das Ergebnis der Tätigkeit im Jahr 2014. Redaktionsschluss für die Beiträge war der 31. Dezember 2014.

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

Inhaltsverzeichnis

1. Keine smartness ohne Freiheit – oder: Wie die Hansestadt Bremen auch als „smart city“ Frei bleiben kann

Der letzte Jahresbericht trug die Überschrift „Big Data für Bond 2.0“ und stand unter dem Eindruck der Enthüllungen von Edward Snowden. Mit dem Zusatz „Für eine menschenrechtliche Einhegung der Nachrichtendienste in Zeiten von Big Data“ versehen, gaben wir diese Überschrift auch dem achten Europäischen Datenschutztag, den Bremen als Vorsitzland des Jahres 2013 der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28. Januar 2014 im Abgeordnetenhaus in Berlin ausrichtete.

Die trotz widriger Wetterverhältnisse über 200 angereisten Teilnehmerinnen und Teilnehmer hörten nach fast acht Monaten andauernder Berichte über massenhafte und anlasslose Überwachungsmaßnahmen von Nachrichtendiensten endlich auch Einschätzungen, die zu Hoffnungen auf die Verbesserung der desolaten Situation für unser Grundrecht auf informationelle Selbstbestimmung Anlass gaben[1]: So konstatierte Erich Möchel, das Internet sei „einfach noch nicht fertig“. Was die Entwicklung von Sicherheitsinfrastrukturen anbelange, sei man in einem sehr frühen Stadium stecken geblieben, was nun endlich nachgeholt werden müsse. Verzicht auf nicht erforderliche Datenerhebungen, Anonymisierung und Verschlüsselung seien die dafür zu beachtenden Grundsätze.

Diesen Grundsätzen müssen wir nicht nur im Zusammenhang mit der Problematik von „Big Data für Bond 2.0“ zum Durchbruch verhelfen. Wir dürfen nicht vergessen, dass Bond 2.0 nicht alleine ist, und das führt uns zu dem Phänomen, das die Überschrift für den Jahresbericht 2014 bilden soll: Bond 2.0 ist unter anderem in Gesellschaft von Preis 2.0, Boss 2.0 und Überwachung 2.0. Da wir beim IT-Gipfel gehört haben, dass wir nicht mehr im 2.0er-Stadium der digitalen Entwicklung sind, sondern es schon um die „Wirtschaft 4.0“ geht, und weil diese Zählerei langsam zu unübersichtlich wird, (wo ist die 3.0 geblieben?), gibt es nun eine neue Kategorie – nämlich die, „smart“ zu sein. Die Wirtschaft 4.0 residiert mit Boss 2.0 und uns in „smart cities“. Diese Zeilen sind der Appell, nicht nur einfach dem Trend zu folgen und aus der Freien eine „smarte“ Hansestadt Bremen zu machen, sondern die Lehren aus dem Jahr 2013 auf IT-Anwendungen zu übertragen, die den klugen Menschen im Land Bremen nützen, ohne ihre Grundrechte zu verletzen.

Das Adjektiv „smart“ bezeichnet im Englischen besonders kluge, pfiffige und intelligente Menschen. Gerade der „Menschenwitz“ ist es also, der mit diesem Begriff auf den Punkt gebracht werden soll. Dieses Kreativitätspotenzial sollen wir uns nach Auffassung derjenigen, die IT-Anwendungen an die Nutzerinnen und Nutzer bringen wollen, nun mit Dingen teilen. Dabei wird im Deutschen aus „smart“ „intelligent“. So haben sich im allgemeinen Sprachgebrauch beispielsweise „smart grids“ (das „intelligente Stromnetz“), „smart ticketing“ („intelligente Fahrkarten“) und der „smart port“ (der „intelligente Hafen“) breitgemacht. Den Dingen wird deshalb „smartness“, also bisher nur Menschen mögliche Kreativität, attestiert, weil sie in der Lage sein sollen, mit Hilfe von Algorithmen, also Rechenprogrammen, menschliches Verhalten „vorauszusagen“. Die Eintrittswahrscheinlichkeit der Prognosen soll deshalb so groß sein, weil es große Datenmengen („Big Data“) sind, in denen die Algorithmen Muster erkennen, die die Grundlagen für die Verhaltensprognosen bilden.

Dabei ist der Begriff „Big Data“ in quantitativer Hinsicht längst nicht mehr zutreffend: Schätzungen zufolge hat die Menschheit gegenwärtig 4,2 Zetabyte Daten produziert. 1 Zetabyte in Byte umgerechnet ergibt eine Eins mit 21 Nullen. Die Datenmenge verdoppelt sich jedes Jahr.[2] Es handelt sich also nicht mehr um „Big Data“, sondern schon längst um „Giant Data“. Daher haben wir es mit Giant Data für „smart prizes“, „smart bosses“, „smart surveillance“ und mit Giant Data für „smart cities“ zu tun. Warum wir dafür kämpfen sollten, dass die Freie Hansestadt Bremen frei bleibt, ohne auf die Vorteile guter IT-Anwendun-

_____

[1] Siehe dazu die Schriftfassungen der Beiträge von Dr. Imke Sommer, Marit Hansen, Professor Dr. Heribert Prantl und Erich Möchel unter https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.9435.de#

[2] http://germany.emc.com/leadership/digital-universe/2012iview/executive-summary-a-universe-of.htm

gen zur Umsetzung der von allen gewollten Pläne zu verzichten, soll im folgenden begründet werden.

1.1 Giant Data für „smart prizes“ – Es gibt keine Gleichheit vor dem Preis

Hannes Grassegger berichtet in der Zeit online[3] unter der Überschrift „Jeder hat seinen Preis“ darüber, dass Big Data es den Anbietern schon gegenwärtig ermöglicht, jeder einzelnen Käuferin einen individuellen Höchstpreis für eine bestimmte Leistung abzuverlangen, also genau den Betrag, den sie gerade noch zu zahlen bereit ist. Das ist der einen oder dem anderen vielleicht schon bei den im Internet angebotenen Hotelpreisen oder Flugpreisen aufgefallen: Wenn die Abfrage für eine gemeinsame Reise vom Rechner der auf dem Land lebenden Schwester aus erfolgt, sieht das Ergebnis anders aus als das der Anfrage, die vom Rechner des in der Großstadt in einem teuren Viertel lebenden Bruders gestartet wird.

Algorithmen speisen sich aus den vorangegangenen Kaufentscheidungen der betreffenden Person und produzieren daraus und aus dem Wissen über das Verhalten vergleichbarer Personen eine Prognose über die persönliche Zahlungsbereitschaft einer Käuferin für ein bestimmtes Produkt zu einem bestimmten Zeitpunkt und an einem bestimmten Ort. Begriffe hierfür sind in den Vereinigten Staaten von Amerika (USA) „price intelligence“ oder „dynamic prices“. Jeder zwanzigste Preis soll nach Grassegger dort bereits personalisiert sein. In Frankreich würden zu ähnlichen Zwecken Preisschilder zunehmend durch Digitalanzeigen ersetzt. Auch in Berlin probiere ein Supermarkt bereits entsprechendes aus. Bei dem beschriebenen Supermarkt werden die Kundinnen und Kunden durch vermeintliche Rabattsysteme zum Mitmachen animiert.

Solange noch analoge Preisschilder mit den „regulären“ Preisen vorhanden sind, lässt sich der persönliche Rabattvorteil überprüfen und scheint auf der Hand zu liegen. Aber spätestens dann, wenn jeder Preis individuell zustande kommt, müsste allen deutlich werden, dass der Vorteil für die Preisgabe der eigenen Konsumdaten nicht mehr erweisbar und damit möglicherweise auch nicht mehr vorhanden ist. Die Logik, nach der sich die Preisdiskriminierung im Wege der Privilegierung derjenigen vollzieht, die mehr oder weniger freiwillig personenbezogene Daten offenbaren, zeigte sich am Ende des Berichtsjahres an einem Rabattsystem, das auf der Preisgabe noch viel sensiblerer personenbezogener Daten beruht: Die Presse berichtete von Planungen des Versicherungskonzerns Generali, für die Berechnung von Prämien für Lebensversicherungen und Krankenversicherungen auf „Fitnessdaten“ zurückgreifen zu wollen. Es solle Preisnachlässe geben, wenn Kundinnen und Kunden der Versicherung ihre Körperdaten, die mit Fitness, Ernährung und Lebensstil und der Einhaltung von Vorsorgeterminen zusammenhingen, zusendeten und so „bewiesen“, dass sie sich in einer Weise verhielten, die von dem Versicherungskonzern als „gesund“ definiert werde.[4]

Spürbare Folge der riesigen Datenberge ist also nicht mehr nur die als besser empfundene, da unserem Geschmack entsprechende Werbung, sondern auch der schlechtere, weil höchstmögliche Preis. Aber auch in anderen elementaren Bereichen sind die Auswirkungen von Giant Data spürbar. Vom Mietvertrag, der wegen eines zudem noch auf unzutreffenden Tatsachen beruhenden Scorewertes nicht zustande kam, berichteten wir bereits (siehe 36. Jahresbericht, Ziffer 15.1). Hinzu kommen die Daten, die unser Auto über unser Fahrverhalten sammelt, für die sich die Kraftfahrzeugversicherung brennend interessiert (siehe dazu die Entschließung der Datenschutzkonferenz „Datenschutz im Kraftfahrzeug – die Automobilindustrie ist gefordert“, Ziffer 19.7). Von den Mautdaten, die möglicherweise demnächst gespeichert werden, ist dabei noch gar nicht die Rede (siehe dazu die Entschließung der Datenschutzkonferenz „Keine Pkw-Maut auf Kosten des Datenschutzes“, Ziffer 19.12).

_____

[3] Ausgabe vom 27.10.2014

[4] Beispielsweise Weser-Kurier vom 22. November 2014 „Mehr Fitness – weniger Prämie – Generali plant verhaltensbasiertes Versicherungsmodell/Datensammlung per Smartphone-App“

1.2 Giant Data für „smart bosses“ – Algorithmen im Arbeitsverhältnis

Auch in dem von der „Wirtschaft 4.0“ geprägten Arbeitsverhältnis wird gesammelt und ausgewertet. Um die Attraktivität der „smarten“ Anwendungen für uns erlebbar zu machen, müssen wir uns in das Denken einer Arbeitgeberin versetzen. Und was wäre geeigneter dafür, als über die deutsche Fußballnationalmannschaft zu sprechen, als deren Chefinnen und Chefs wir uns ja vermutlich fast alle fühlen?

Nachdem Deutschland im Sommer 2014 den Fußballweltmeistertitel erhalten hatte, kam die Frage auf, wie viel Anteil daran Big Data gebühre.[5] Hintergrund dieser Frage ist die Partnerschaft zwischen dem Deutschen Fußballbund e. V. und der IT-Firma SAP. Die Firma hatte eine Datenbank mit Daten wie Laufwegen, Raumaufteilungen und Ballbesitz von über 7.000 Spielen der potenziellen Gegner der deutschen Nationalmannschaft gefüllt, die per Algorithmen ausgewertet werden konnten. Wer genau weiß, in welchen Situationen selbst ein Christiano Ronaldo Fehler macht, scheint den Titel schon halb in der Tasche zu haben. Auch in der Bundesliga soll Giant Data eingesetzt werden. So plant die FC Bayern München AG, mithilfe derselben IT-Firma Daten über das Leistungsvermögen, die Stärken und Schwächen, insbesondere die Gesundheit der Spieler zu erfassen und in Echtzeit auszuwerten. Ziel ist es, „einen neuen, optimierten Spieler“ zu schaffen.[6] Dieselbe IT-Firma hat übrigens auch eine Partnerschaft mit der TSG 1899 Hoffenheim Fußball-Spielbetriebs GmbH. Dort tragen Spieler Trikots, in die Sensoren eingebaut sind, deren Daten dem Trainer auf eine Datenbrille gespielt werden.

Die schöne neue Fußballwelt ist vermutlich nur ein Vorbote dessen, was auch sonst in der Arbeitswelt geplant ist. Die Fragen, welche Daten der Beschäftigten Arbeitgeber verarbeiten dürfen und was mit diesen Daten bei Vereinswechsel beziehungsweise Arbeitsplatzwechsel passiert, werden vom Bundesdatenschutzgesetz eindeutig beantwortet: Datenverarbeitung im Beschäftigungsverhältnis, also auch Giant Data für „smart bosses“, muss sich im Rahmen des § 32 Bundesdatenschutzgesetz halten. Danach dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, „wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.“ Von wirtschaftlichem oder sportlichem Erfolg, der durch Datenverarbeitungen gefördert werden soll, steht da nichts. Nach Beendigung des Beschäftigungsverhältnisses muss der Arbeitgeber die persönlichen Daten der ehemaligen Beschäftigten selbstverständlich löschen, weil der Zweck, für den sie erhoben wurden, weggefallen ist. Da also keine gesetzliche Grundlage für Giant Data für „smart bosses“ zu finden ist, bleibt nur die Einwilligung des Betroffenen als Rechtfertigungsgrund für den Grundrechtseingriff. Das Arbeitsverhältnis enthält ein hierarchisches Gefälle, das die Freiwilligkeit von Einwilligungen grundsätzlich infrage stellt und auch im Verhältnis zwischen hoch verdienenden Bundesligaprofis und ihren Vereinen muss an die Freiwilligkeit von Einwilligungen ein Fragezeichen gesetzt werden. Auch sehr gut bezahlte Menschen handeln nicht unbedingt freiwillig, wenn sie in einem Abhängigkeitsverhältnis stehen.

Für uns als Chefinnen und Chefs der Nationalmannschaft sind diese Antworten unbefriedigend, weil sie die Rechtmäßigkeit der Datenerhebungen in Zweifel ziehen und den Erfolg im Fußball deshalb vermeintlich erschweren. Ebenso scheinen die geltenden Regeln des Beschäftigtendatenschutzes aus Sicht der Chefinnen und Chefs der „Wirtschaft 4.0“ den wirtschaftlichen Erfolg zu hemmen. An dieser immer weiter um sich greifenden Einschätzung zeigt sich, wie gefährdet der gesellschaftliche Konsens über Beschäftigtendatenschutz ist. Der Dammbruch in Sachen Giant Data im Fußballsport, den wir als Fans gutheißen mögen, kann uns an anderer Stelle also zumindest nasse Füße bereiten.

_____

[5] Christian Scholz, http://blogs.faz.net/personal-blog/2014/08/26/big-data-grosse-glaeserne-mitarbeiter-408/

[6] http://www.handelsblatt.com/technologie/vernetzt/big-data-im-sport-der-glaeserne-lahm/10707508.html

1.3 Giant Data für „smart surveillance“ – Dürfen uns Algorithmen überwachen?

Dass Begriffe, die mit dem Attribut „smart“ verbundenen werden, häufig merkwürdige Konnotationen haben, wird an dem EU-Projekt „smart surveillance“ deutlich, in dem ich im Berichtsjahr eingeladen war, zu gesetzlichen Anforderungen an die „intelligente Überwachung“ Stellung zu nehmen.[7] Wie schon dargelegt, ist „Smartness“ eine Eigenschaft, die zutiefst Menschliches bezeichnet, das allgemein als positiv anerkannt ist. „Smarte“ Menschen sind kreativ, unkonventionell, überraschend und empathisch. Qua definitionem können Algorithmen, also einem binären Code folgende Softwareprogramme weder kreativ, unkonventionell, überraschend noch empathisch sein. Das Attribut „smart“ passt also eigentlich nicht für Algorithmen. Der von dem EU-Projekt mit der „smartness“ in Verbindung gebrachte Begriff „surveillance“, also Überwachung, zielt auf die Beobachtung menschlichen Verhaltens mit dem Ziel, abweichendes Verhalten zu erkennen. Wie die Reaktionen auf die Enthüllungen Edward Snowdens zeigen, wird Überwachung von der überwiegenden Mehrheit der Menschen negativ bewertet.[8] Insofern erscheint der Begriff einer „smarten“ Überwachung sowohl zynisch und als auch missverständlich.

Diese Schrägheit des Begriffes hat aber auch etwas Gutes, denn sie weist auf wesentliche Mindestanforderungen, die gesetzliche, verfassungsrechtliche und mit der Europäischen Grundrechtecharta in Einklang stehende Regelungen zu dem Phänomen „smart surveillance“, aber auch allen anderen Spielarten „smarter“ Anwendungen auf jeden Fall beinhalten müssen: Einerseits folgt aus der Erkenntnis, dass nur Menschen „smart“ sein können, dass sichergestellt sein muss, dass grundrechtsrelevante Entscheidungen Menschen vorbehalten bleiben müssen und nicht von Algorithmen getroffen werden dürfen. Andererseits muss dabei der kreative und freie Aspekt der menschlichen „smartness“ gewährleistet sein: Menschen dürfen keine negativen Folgen befürchten müssen, wenn ihre Entscheidung eine andere ist als diejenige Entscheidung, die der Algorithmus „vorschlägt“.

1.4 Giant Data für „smart cities“ – Warum aus der „Freien“ nicht die nur vermeintlich „smarte“ Hansestadt Bremen werden sollte

„Smart city“ („intelligente Stadt“) ist also der Name, unter dem Giant Data in die Stadt kommt.[9] Dieser Begriff steht nicht nur für riesige Datenmassen, sondern auch für ein riesiges Geschäftsfeld: Die Süddeutsche Zeitung zitierte am 14. Mai 2014 die Schätzung einer Marktforschungsfirma, die davon ausging, dass im Jahr 2014 weltweit 190 Milliarden Euro in Smart-City-Projekte fließen würden. Hierbei ist zu beachten, dass viele in solche Projekte involvierte Unternehmen im Hinblick darauf, dass sich ihre Aufwendungen später erheblich auszahlen werden, den Kommunen für ihre Beteiligung nichts berechnen, also scheinbar selbstlos mitwirken.

Die Ziele von „smart cities“ sind einleuchtend und zeitgemäß. Sie reagieren auf den Umstand, dass seit dem Ende der letzten Dekade die Hälfte der Weltbevölkerung in urbanen Gebieten lebt. Vor dem Jahr 2025 soll dieser Prozentsatz weltweit gesehen auf 60 Prozent ansteigen. An den Städten Brüssel, Seoul, Bogota ist nach Sarwant Singh ablesbar, dass es Städte gebe, die wichtiger als ihre Nationalstaaten seien, auch deshalb, weil Städte zu über 40 Prozent zum Bruttosozialprodukt beitrügen.[10] Diese Entwicklung bedeutet für die Verwaltungen der Städte große Herausforderungen in sozialer, wirtschaftlicher und ökologischer Hinsicht. Die Konzepte zur „smart city“ verheißen hierfür Lösungen, wobei die sozialen Herausforderungen eher im Hintergrund bleiben. So heißt es in Hamburg: „Die smart city, also die vernetzte und kluge Stadt, verbessert die Lebensqualität der Men-

_____

[7] Siehe www.smartsurveillance.eu

[8] Im Juni 2014, also genau ein Jahr nach Veröffentlichung der ersten Enthüllungen, befürwortete laut ZDF-Politikbarometer die überwiegende Mehrheit der Deutschen (82 %) die Enthüllungen Edward Snowdens. Die freiheitseinschränkende Bedeutung des Begriffes Überwachen wird auch von Foucault verwendet, Michel Foucault „Surveiller et punir“ (Michel Foucault, 1975)

[9] Kongress „Die Intelligente Stadt“ der Stiftung Lebendige Stadt http://www.lebendige-stadt.de/web/template2neu.asp?sid=565&nid=&cof=212

[10] Sarwant Singh in: Forbes 6/19/2014

schen durch intelligente, innovative Infrastrukturen, die helfen, Mobilität effizienter zu machen, Ressourcen zu schonen und negative Umwelteinflüsse zu reduzieren.“ Es gehe darum „Antworten auf die Fragen nach Mobilität, öffentlicher Infrastruktur, Service, Energieverbrauch, Schadstoffausstoß und Lebensqualität (zu) finden.“[11] Natürlich gehören in diesen Zusammenhang die „smart grids“ (intelligente Stromnetze), das Stromerzeuger, Stromspeicher und elektrische Verbraucher miteinander vernetzt und steuert, um ihre Effizienz zu optimieren.

Diese schon seit einigen Jahren diskutierte Entwicklung war aber erst der Anfang. Nach Sarwant Singh gehören zur „smart city“ die „smart governance“, „smart healthcare“, „smart education“, „smart buildings“, „smart mobility“, „smart infrastructure“, „smart technology“, „smart energy“ und sogar der „smart citizen“ (also „intelligentes“ Regieren und Gesundheitssystem, „intelligente“ Gebäude, „intelligente“ Erziehung, Mobilität, Technologie und Energie und „intelligente“ Bürgerinnen und Bürger). Da bleibt kein Datenwunsch für kein Geschäftsmodell offen. Gesundheitsdaten fließen ebenso wie Umweltdaten in den gigantischen Smart-City-Datenberg und werden von Algorithmen, die von den größten IT-Unternehmen der Welt verantwortet werden, nach Kriterien ausgewertet, die für uns alle undurchsichtig sind. Der Datenhunger der „smart cities“ ist unersättlich. Weil sie auch vor personenbezogenen Daten nicht Halt machen, ist hiervon das Grundrecht auf informationelle Selbstbestimmung tangiert.

Auch Bremen muss sich den Herausforderungen an Städte des 21. Jahrhunderts stellen und dabei selbstverständlich auch IT-Anwendungen einsetzen. Aber die Freiheit der Hansestadt sollte dabei nicht aufs Spiel gesetzt und Kollisionen mit dem Grundrecht auf informationelle Selbstbestimmung von vornherein vermieden werden. Deshalb sollten nur solche IT-Anwendungen eingesetzt werden, die die Prinzipien beachten, mit deren Hilfe „smartness“ vom Problem zur Lösung werden kann: Datensparsamkeit, Anonymisierung und Verschlüsselung.

1.5 Datensparsamkeit, Anonymisierung und Verschlüsselung als konstitutive Prinzipien einer Freien „smarten“ Hansestadt Bremen

Die kurzen Aufrisse über „smarte“ Preise, Arbeitgeber, Überwachung und Städte zeigen die Möglichkeiten, aber auch die Gefahren, die Algorithmen im Zeitalter von Giant Data bergen, wenn sie sich auch auf personenbezogene, und damit zu Profilen kumulierbare Daten beziehen. Dr. Joël Cachelin bringt dies folgendermaßen auf den Punkt: „Die Analyse der Vergangenheit ermöglicht die Antizipation der Zukunft. Der Supermarkt weiß aufgrund kumulierter Einkäufe, wann eine Frau schwanger ist. Der Arbeitgeber erkennt Burnouts, Facebook Homosexualität, Google einen Seitensprung – noch vor uns. Unternehmen versuchen negative Risiken der Zukunft bereits heute durch die Analyse der Vergangenheit zu erkennen. Eine Mitarbeiterin wird entlassen, weil ihr Surfverhalten auf das Frühstadium einer psychischen Erkrankung hinweist. Krankenkassen und Versicherungen weisen Kunden ab, weil sie in der Vergangenheit zu viele Risiken eingegangen sind. Prognosen helfen, mögliche Risiken zu erkennen, erhöhen die Planbarkeit und die wahrgenommene Sicherheit, schränken aber auch den Zufall und die Freiheit ein.“[12]

Um diesen Gefahren zu begegnen brauchen „smarte“ Anwendungen demokratische Regulative. Die gibt es bereits. Das Grundgesetz formuliert für „smart cities und Co.“ wichtige Grundsätze. Schon in seinem Volkszählungsurteil wies das Bundesverfassungsgericht auf das hin, was wir heute als die grundsätzlichen Probleme von Profilbildungen kennen: „Durch die Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten der Informationstechnologien kann ein für sich alleine als belanglos beurteiltes Datum einen neuen Stellenwert bekommen.“ Mit seiner daraus abgeleiteten Erkenntnis, eine abstrakte

_____

[11] http://www.hamburg.de/smart-city/nofl/4379852/2014-09-25-smart-city-summit/

[12] Dr. Joël Cachelin, Die Zukunft nimmt die Gegenwart gefangen, www.schattenzeitalter.ch

Einteilung in schützenswerte und freizugebende Daten sei nicht mehr möglich, war das Bundesverfassungsgericht 1983 geradezu prophetisch.

Im Volkszählungsurteil hat das Bundesverfassungsgericht neben diesen weisen Worten zum sehr weit zu fassenden Schutzbereich des Grundrechtes auf informationelle Selbstbestimmung auch die Grenzen dieses Grundrechtes beschrieben, das wie alle anderen mit den anderen Grundrechten und Verfassungsgrundsätzen in ein Verhältnis der praktischen Konkordanz gebracht werden muss. In das Grundrecht auf informationelle Selbstbestimmung darf danach eingegriffen werden, wenn sich dieser Eingriff auf ein Gesetz oder eine Einwilligung stützen kann. Nach einhelliger Auffassung der einschlägigen Kommentare zum Bundesdatenschutzgesetz ist „Data Mining" als der begriffliche Vorgänger von „smarter" Giant Data weder für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich noch bietet das Bundesdatenschutzgesetz eine sonstige Rechtsgrundlage. Data Mining sei „Systematische Zweckentfremdung", verstoße daher gegen das Postulat der Zweckbindung und könne daher nicht aus dem Gesetz gerechtfertigt werden. Wegen der fehlenden gesetzlichen Grundlage könne daher nur die Einwilligung der Betroffenen entsprechende Datenverarbeitungen rechtfertigen.[13] Eine wirksame Einwilligung wird bei fast allen „smarten" Anwendungen fehlen.

Was bleibt, um „smart cities und Co." mit dem Grundrecht auf informationelle Selbstbestimmung in Einklang zu bringen, sind Datensparsamkeit („privacy by design") und die wirksame Anonymisierung. Für Daten, für deren Verarbeitung sich doch eine Rechtsgrundlage oder eine wirksame Einwilligung finden, kommen darüber hinaus die Verschlüsselung und andere technische und organisatorische Maßnahmen des Datenschutzes in Betracht. Diese drei Grundsätze Datenvermeidung, Anonymisierung und Verschlüsselung und alle anderen Maßnahmen des technischen und organisatorischen Datenschutzes sind technikneutral und finden ihre Grundlage in der Grundrechtstheorie. Sie bringen auch aus heutiger Sicht alle erforderlichen Regelungen für den Umgang mit „smarten" Anwendungen auf den Punkt.

Das in diesem Zusammenhang gegen diese Prinzipien angeführte Argument, das Datenschutzrecht und die ihm zugrunde liegenden Grundsätze seien „alt" und deshalb von der technischen Entwicklung überholt, ist unzutreffend. Zunächst einmal ist das Datenschutzrecht zwar nicht die neueste Rechtsmaterie, aber es ist technikneutral formuliert und gilt daher auch für jede neue technische Entwicklung. Und dass am Ende von Normierungsvorhaben, wie sie jetzt in Europa diskutiert werden, keine Regelungen stehen werden, die solche Geschäftsmodelle im Nachhinein legalisieren, die Grundrechte verletzen, versteht sich von selbst. Gegenstand von Novellierungen kann also nur die Konkretisierung der Grundsätze, nicht jedoch ihre Veränderung sein. Auch die Datenschutz-Grundverordnung wird sich an der Europäischen Grundrechtecharta messen lassen müssen. Ob es gelungen ist, diesen Maßstäben zu genügen, wird letztlich der Europäische Gerichtshof entscheiden, der uns im Berichtsjahr mit zwei grundlegenden und sehr datenschutzfreundlichen Entscheidungen erfreute (siehe Entschließungen der Datenschutzkonferenz zum „Ende der Vorratsdatenspeicherung in Europa!", Ziffer 19.6 und „Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen", Ziffer 19.10).

1.5.1 Datensparsamkeit – keine unnötigen personenbezogenen Daten erheben

Für die legitimen Ziele von „smarten" Anwendungen ist der Personenbezug häufig irrelevant. In diesen Fällen kann der „Beifang" personenbezogener Daten reduziert werden, ohne die legitimen Ziele aufzugeben. Dies ist Ausdruck des Prinzips der Datensparsamkeit, dessen Gedanken auch unter den Begriffen Datenvermeidung und „privacy by design" formuliert sind. Dass dieser so notwendige Verzicht auf die Erhebung und Verarbeitung personenbezogener Daten in der Realität so schwer durchzusetzen ist, liegt auch daran,

[13] Simitis, Bundesdatenschutzgesetz, § 3 Randnummer 72

dass die Erhebung und Speicherung von personenbezogenen Daten bis zu dem Zeitpunkt, zu dem sie für ein künftiges Geschäftsmodell einmal nützlich sein könnten, einerseits kaum Kosten verursacht und der Markt mit „smarten“ Anwendungen andererseits hohe Umsätze verspricht. Die 190 Milliarden Euro, die Schätzungen zufolge im Berichtsjahr in „Smart-City-Projekte“ flossen, wurden schon genannt. Der Jahresumsatz der im Zusammenhang mit den Sporterfolgen durch Giant Data erwähnten IT-Firma SAP betrug im Jahr 2013 ganze 16,815 Milliarden Euro. Wie die Debatte über die Europäische Datenschutz-Grundverordnung zeigt, sehen sich alle, die in Europa auf hohe Grundrechtsstandards pochen, vermutlich auch deshalb einer starken Lobby gegenüber (siehe dazu 35. Jahresbericht, Ziffer 1.2 und 36. Jahresbericht, Ziffer 22.2), weil ihr Erfolg die Realisierung dieser hohen Gewinnerwartungen gefährden könnte.

In dieselbe Richtung wie diese Lobbybestrebungen auf europäischer Ebene geht in Deutschland ein verfassungsrechtlicher Ansatz, der den genannten Erkenntnissen des Bundesverfassungsgerichtes im Volkszählungsurteil entgegensteht. Danach sollen „unbedeutende“ personenbezogene Daten einfach aus dem Schutzbereich des Grundrechtes herausdefiniert und bestimmte Verarbeitungen personenbezogener Daten ohne Betrachtung des Einzelfalles und ohne Abwägung der widerstreitenden Interessen im Einzelfall pauschal erlaubt werden.[14] Solchen Bestrebungen kann eine weitere Aussage des Bundesverfassungsgerichts aus dem Volkszählungsurteil entgegengehalten werden: „Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss.“ Das gilt selbstverständlich auch dann, wenn die Freiheitswahrnehmung von privater Seite bedroht ist.

1.5.2 Anonymisierung – den Personenbezug erfolgreich und nachhaltig kappen

Das Grundrecht auf informationelle Selbstbestimmung schützt nur personenbezogene Daten, also Daten, die mit einer bestimmten Person in Zusammenhang gebracht werden können. Pseudonymisierte Daten, also solche Daten, die einer Person zugeordnet werden, die lediglich unter einem anderen als ihrem gewöhnlichen Namen oder unter einer Nummer erfasst wird, sind deshalb weiterhin personenbezogene Daten. Erst wenn der Personenbezug nicht mehr hergestellt werden kann, Daten also wirksam anonymisiert sind, fallen sie aus dem Schutzbereich des Grundrechtes auf informationelle Selbstbestimmung heraus.

Für viele „smarte“ Anwendungen sind nicht identifizierbare Personen, sondern Personengruppen interessant. Daher können in diesen Fällen anonymisierte Daten verwendet werden. Was zu tun ist, um zuvor personenbezogene Daten erfolgreich zu anonymisieren, legt das Bundesdatenschutzgesetz fest: „Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.“

1.5.3 Zugangserschwerungen durch Verschlüsselung und Co.

Wenn es wider Erwarten doch eine Rechtsgrundlage für Datenverarbeitungen im Rahmen von „smarten“ Anwendungen geben sollte, muss auf jeden Fall sichergestellt werden, dass nur diejenigen die Daten tatsächlich verarbeiten können, denen die Datenverarbeitung erlaubt ist. Kryptografische Schutzverfahren erschweren die Zugänglichkeit von Daten am sichersten. Schon einfache Sicherheitsmaßnahmen (wie die Verschlüsselung von Internetseiten, „https“ statt „http“) steigern die Komplexität und die Kosten von Angrif-

_____

[14] Beispielsweise die Äußerungen von Professor Pernils, http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/08/expertenrunde-big-data.html

fen. Hinweise zur Verschlüsselung elektronischer Kommunikation finden sich auf der Internetseite des Bundesamtes für Sicherheit in der Informationstechnik.[15] Daneben listen das Bremische Datenschutzgesetz und das Bundesdatenschutzgesetz technische und organisatorische Maßnahmen auf, die es erschweren, Zugang zu personenbezogenen Daten zu erhalten. Hierbei handelt es sich um die Maßnahmen Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle und Verfügbarkeitskontrolle.

1.6 Transparenz und das Erfordernis freier menschlicher Letztentscheidungen als unhintergehbare Voraussetzungen für den Einsatz von Algorithmen

Algorithmen sind Ausdruck der individuellen Realitätswahrnehmung also auch eventuell vorhandener Vorurteile, die diejenigen, die sie programmieren, zu einer bestimmten Zeit an einem bestimmten Ort haben. Algorithmen sind also nicht dynamisch und nicht demokratisch legitimiert. Deshalb brauchen wir Transparenz über Algorithmen. Wir müssen wissen, welche unserer Daten in die Algorithmen einfließen und wie sie gewichtet werden. Dies muss im Bundesdatenschutzgesetz ausdrücklich klargestellt werden.

Am 17. Dezember 2014 fasste die Bürgerschaft (Landtag) einstimmig Beschlüsse, der diesem Erfordernis Rechnung tragen. Die Bremische Bürgerschaft setzte sich darin für eine bremische Bundesratsinitiative zur Stärkung der Rechte von Verbraucherinnen und Verbrauchern gegenüber Auskunfteien ein. Der Senat solle im Bundesrat eine Novellierung des § 34 Absatz 4 Satz 1 Bundesdatenschutzgesetz initiieren, nach der vom Auskunftsrecht der Verbraucherinnen und Verbraucher ausdrücklich auch die Gewichtung der zur Berechnung des Scoring-Wertes verwendeten Daten umfasst ist. Soweit die Offenlegung konkreter Gewichtungsdaten und Berechnungsdaten die Wahrung des Geschäftsgeheimnisses von Auskunfteien unzulässig beeinträchtige, seien geeignete andere, für Betroffene aussagekräftige Informationen, beispielsweise die Nennung der Rangfolge der genutzten Daten zu definieren. Darüber hinaus müsse gesetzlich klarer gefasst werden, welche Daten zur Berechnung eines Scoring-Wertes herangezogen werden dürften. Jedenfalls müsse ausgeschlossen werden, dass das Wohnumfeld für die Berechnung des Scoring-Wertes herangezogen werden dürfe.

Diese Beschlüsse der Bremischen Bürgerschaft sind deshalb so wichtig, weil der Bundesgerichtshof im Berichtsjahr feststellte, dass Verbraucherinnen und Verbraucher gegenüber der Wirtschaftsauskunftei Schufa lediglich einen Anspruch auf die Offenlegung der in den Algorithmus eingehenden Datenarten hätten. Der Algorithmus selbst sei als Geschäftsgeheimnis der Schufa von der Transparenzpflicht ausgenommen (siehe dazu Ziffer 14.1 dieses Berichts). Dies Ergebnis durch eine Gesetzesänderung zu korrigieren, wäre ein wichtiger Schritt auf dem Wege zu grundrechtsverträglichen „smarten“ Anwendungen.

Aus der Erkenntnis, dass nicht Algorithmen, sondern nur Menschen „smart“ und intelligent sein können, folgt die schon genannte unhintergehbare Forderung für „smarte“ Giant-Data-Anwendungen: Algorithmen dürfen keine Letztentscheidungen treffen, denn sie sind Menschenwerk und Irren ist menschlich. Sofern es sich um Entscheidungen mit Grundrechtsrelevanz handelt, muss der menschliche Fehler, den ein Algorithmus möglicherweise birgt, zum Zeitpunkt der zu treffenden Entscheidung von einem anderen Menschen ersetzt werden können. Nur so können Vorurteile korrigiert und neue, zum Zeitpunkt der Programmierung noch nicht vorhersehbaren Entwicklungen in die Entscheidung einfließen. Diese letztlich entscheidenden Menschen müssen in ihrer Entscheidung frei sein. Dies hat zusätzlich zur Voraussetzung, dass sie keine Nachteile zu befürchten haben, wenn sie den „Vorschlägen“ der Algorithmen nicht folgen.

_____

[15] https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/Verschluesseltkommunizieren/verschluesselt_kommunizieren_node.html

1.7 Wie die Hansestadt Bremen auch als „smart city“ Frei bleiben kann

Die Freie Hansestadt Bremen kann „smarte“ Anwendungen mit ihren verlockenden Angeboten für Nachhaltigkeit also durchaus nutzen, ohne die Grundrechte der Bremerinnen und Bremer zu verletzen, wenn die Erhebung personenbezogener Daten vermieden, und personenbezogene Daten – deren Erhebung unvermeidbar ist – wirksam anonymisiert werden. Der Zugang zu den Daten muss durch Verschlüsselungen und andere Maßnahmen des technischen und organisatorischen Datenschutzes erschwert und gesteuert werden. Die auf diese Weise veränderten Datenberge kann die Freie Hansestadt Bremen getrost solchen Algorithmen zur Verfügung stellen, deren Annahmen und „Vorurteile“ die Menschen im Land Bremen kennen und richtig finden. Wenn die „errechneten“ Entscheidungsvorschläge der Algorithmen im grundrechtsrelevanten Bereich dann noch Menschen vorgelegt werden, die frei darüber entscheiden können, ob sie diesen Vorschlägen folgen, kommt die auf diese Weise gezähmte „smarte“ Giant Data den intelligenten Bremerinnen und Bremern zugute.

Wenn uns dies gelingt, können wir statt in einer vermeintlich „smarten“ Hansestadt Bremen weiter in unserer Freien Hansestadt Bremen leben, ohne auf die Vorteile von Algorithmen zu verzichten, denen wir genau das beibringen, was die Menschen im Land Bremen für richtig und gerecht halten.

Dr. Imke Sommer

2. Bremische Bürgerschaft

2.1 Ergebnisse der Beratungen des 36. Jahresberichts

Bericht und Antrag des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zum 36. Jahresbericht der Landesbeauftragten für Datenschutz vom 21. März 2014 (Drucksache 18/1320) und zur Stellungnahme des Senats vom 12. August 2014 (Drucksache 18/1521)

I. Bericht

Die Bürgerschaft (Landtag) überwies in ihrer Sitzung am 21. Mai 2014 den 36. Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit vom 21. März 2014 (Drucksache 18/1320) und in ihrer Sitzung am 24. September 2014 die dazu erfolgte Stellungnahme des Senats vom 12. August 2014 (Drucksache 18/1521) an den Ausschuss für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zur Beratung und Berichterstattung.

Der Ausschuss stellte bei den nachfolgend aufgeführten Punkten des 36. Jahrsberichts Beratungsbedarf fest:

Ziffer 3.2 Mangelnde Beteiligung behördlicher Datenschutzbeauftragter

Ziffer 4.3 Sichere Administrationsumgebung Dataport

Ziffer 4.4 Rahmendatenschutzkonzept BASIS.Bremen

Ziffer 5.1 Telekommunikationsüberwachung durch die Polizeien

Ziffer 5.3 Speicherung personenbezogener Daten bei der Polizei

Ziffer 5.4 Erweiterung der Anwendung INPOL und INPOL-Land

Ziffer 5.8 Rahmendatenschutzkonzept der Polizei Bremen

Ziffer 5.6 Aktuelle Situation im Stadtamt

Ziffer 5.9 Rahmendatenschutzkonzept des Senators für Inneres und Sport

In seiner Sitzung am 24. Oktober 2014 erörterte der Ausschuss die beratungsbedürftigen Punkte mit der Landesbeauftragten für Datenschutz und Informationsfreiheit und Vertretern der betroffenen Ressorts.

Zu den einzelnen Punkten nimmt der Ausschuss für Wissenschaft, Medien, Datenschutz und Informationsfreiheit wie folgt Stellung:

Ziffer 3.2 Mangelnde Beteiligung behördlicher Datenschutzbeauftragter

Der Ausschuss begrüßt, dass im konkreten Fall eine Einigung erzielt worden ist. Der Ausschuss stellt jedoch fest, dass grundsätzlich bei der Einbeziehung der behördlichen Datenschutzbeauftragten und der Kooperation zwischen der Landesbeauftragten für Datenschutz und den öffentlichen Dienststellen ein Optimierungsbedarf besteht.

Der Ausschuss fordert daher alle öffentlichen Dienststellen auf, ihre behördlichen Datenschutzbeauftragten künftig rechtzeitig und umfassend in die Verfahren einzubeziehen und in datenschutzrechtlichen Fragen besser mit der Landesbeauftragten zusammenzuarbeiten.

Ziffer 4.3 Sichere Administrationsumgebung Dataport

Ziffer 4.4 Rahmendatenschutzkonzept BASIS.Bremen

Der Ausschuss stellt fest, dass im Vergleich zum Vorjahresbericht zwar Verbesserungen erzielt worden sind, jedoch immer noch nicht alle notwendigen Konzepte und Verfahrens-

beschreibungen vollständig vorliegen. Eine Strukturanalyse und Risikoanalyse ist nach wie vor nicht erfolgt. Die Senatorin für Finanzen hat dem Ausschuss versichert, dass an den erforderlichen Dokumenten gearbeitet und diese der Landesbeauftragten für Datenschutz so bald wie möglich vorgelegt werden.

Zum Einsatz von Dataport bekräftigt der Ausschuss seine Forderung, dort ausschließlich vertrauenswürdiges und verlässliches Personal zu beschäftigen und die Anzahl der Personen, die Zugriff auf die Daten haben, auf ein Minimum zu beschränken. Der Einsatz von externen Dienstleistern sollte eng begrenzt und strengen Regelungen unterworfen sein. Dataport sollte versuchen, das erforderliche Know-how im eigenen Unternehmen aufzubauen und vorzuhalten.

Ziffer 5.1 Telekommunikationsüberwachung durch die Polizeien

Ziffer 5.3 Speicherung personenbezogener Daten bei der Polizei

Ziffer 5.4 Erweiterung der Anwendung INPOL und INPOL-Land

Ziffer 5.8 Rahmendatenschutzkonzept der Polizei Bremen

Der Ausschuss kritisiert die zum Teil erheblichen Defizite bei der Umsetzung der datenschutzrechtlichen Anforderungen bei der Polizei Bremen, zumal die Forderungen der Landesbeauftragten für Datenschutz im Wesentlichen anerkannt werden und keine größeren, inhaltlichen Dissense bestehen. Die unzureichende Umsetzung liegt nach Auskunft der Polizei und des Senators für Inneres und Sport vor allem daran, dass der Polizei für diese Aufgaben nicht genügend Personal zur Verfügung steht.

Der Ausschuss hält diesen Verweis auf fehlendes Personal für nicht akzeptabel, da es sich bei den datenschutzrechtlichen Anforderungen um gesetzliche Verpflichtungen handelt, denen öffentliche Stellen nachzukommen haben. Die Erledigung der damit verbundenen Aufgaben muss sichergestellt werden.

Der Ausschuss sieht es hingegen als positive Entwicklung, dass die Polizei einen eigenen Datenschutzbeauftragten hat, an den sich die Bürgerinnen und Bürger nunmehr direkt wenden können. Dieser verfügt auch über eine eigene Homepage, auf der eine Vielzahl an Informationen bereitgestellt wird.

Ziffer 5.6 Aktuelle Situation im Stadtamt

Ziffer 5.9 Rahmendatenschutzkonzept des Senators für Inneres und Sport

Der Ausschuss begrüßt, dass im Stadtamt inzwischen die Stelle des behördlichen Datenschutzbeauftragten besetzt worden ist. Aufgrund der langen Zeit nicht erfolgten Besetzung der Stelle sind jedoch viele Aufgaben im Bereich des Datenschutzes unerledigt geblieben.

Der Ausschuss erinnert daran, dass es sich beim Datenschutz um gesetzliche Verpflichtungen handelt, die umgesetzt werden müssen. Er bittet daher den Senator für Inneres und Sport, für eine zügige Abarbeitung zu sorgen und zu gewährleisten, dass die Einhaltung der datenschutzrechtlichen Vorgaben im Bereich des Stadtamtes künftig sichergestellt wird.

Gleiches gilt für die Behörde des Senators für Inneres und Sport. Der Ausschuss kritisiert, dass die Arbeiten an dem Rahmendatenschutzkonzept nach wie vor nicht abgeschlossen sind. Er fordert den Senator für Inneres und Sport daher auf, dieses zeitnah vorzulegen.

Der Ausschuss hat diesen Bericht einstimmig beschlossen.

II. Antrag

Die Bürgerschaft (Landtag) möge beschließen:

Die Bürgerschaft (Landtag) tritt den Bemerkungen des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit bei.

3. Behördliche Beauftragte für den Datenschutz

3.1 Gesetzeskonforme Bestellung behördlicher Datenschutzbeauftragter

Wiederholt waren wir im Berichtsjahr mit Fragen beschäftigt, die die gesetzeskonforme Bestellung behördlicher Datenschutzbeauftragter durch die dem Bremischen Datenschutzgesetz unterliegenden Stellen betrafen. Besonderen Raum nahm dabei erneut die Bestellung eines externen Datenschutzdienstleistungsunternehmen zum Beauftragten ein. In diesem Zusammenhang befassten wir uns mit dem Inhalt von Dienstleistungsverträgen, die die Bestellung einer beziehungsweise eines externen Datenschutzbeauftragten zum Gegenstand hatten. Wir wiesen hierzu darauf hin, dass auch im Hinblick auf die Tätigkeit einer beziehungsweise eines externen behördlichen Datenschutzbeauftragten die Bestimmungen des § 7a Bremisches Datenschutzgesetz, der für die Bestellung und die Tätigkeit der Amtsinhaberin oder des Amtsinhabers allein maßgeblich ist, einzuhalten sind. Die oder der behördliche Datenschutzbeauftragte muss ihre beziehungsweise seiner sich aus der Gesetzesvorschrift ergebenden Aufgaben weisungsfrei und in vollem Umfang wahrnehmen können. Soll im Hinblick auf die Vergabe der Funktion an eine externe Person ein Geschäftsbesorgungsvertrag abgeschlossen werden, so muss dieser den Anforderungen des § 7a Bremisches Datenschutzgesetz entsprechen. In den Fällen, in denen sich eine dienststelleninterne Lösung nicht finden ließ, empfahlen wir daher, die Verträge an die Gesetzesbestimmungen anzupassen und machten entsprechende Änderungsvorschläge.

Bereits in unserem 35. und 36. Jahresbericht hatten wir über die Nichtbestellung einer oder eines neuen behördlichen Datenschutzbeauftragten durch eine große bremische Behörde mit zahlreichen Verfahren personenbezogener Datenverarbeitung berichtet. Die Nichtbestellung war von uns gegenüber dem zuständigen Senator beanstandet worden. Die Neubestellung ließ auch im Berichtsjahr noch längere Zeit auf sich warten. Bis dahin häuften sich bei uns die Beschwerden von Bürgerinnen und Bürgern, die sich beklagten, bei der betreffenden Behörde keine Ansprechpartnerin beziehungsweise keinen Ansprechpartner für ihr datenschutzrechtliches Anliegen zu finden. Begründet wurde die Nichtbestellung auch weiterhin mit dem in der Behörde stattfindenden Reorganisationsprozess, der eine schnellere Wiederbesetzung des Amtes nicht zulasse. Schließlich wurde die Funktion im Oktober 2014 befristet für den Zeitraum eines Jahres besetzt. Die Behörde gab an, die zentrale Wahrnehmung der Aufgaben der oder des behördlichen Datenschutzbeauftragten durch die senatorische Dienststelle des betreffenden Ressorts weiterhin zu prüfen.

3.2 Weiterbeschäftigung des Datenschutzbeauftragten trotz Personalabbaus

Beratungsanfragen im Berichtsjahr geben Anlass, die rechtlichen Voraussetzungen der Amtsbeendigung von behördlichen Datenschutzbeauftragten zu erläutern.

Der Betriebsrat einer bremischen Gesellschaft wandte sich mit dem Hinweis an uns, dass dort auch der behördliche Datenschutzbeauftragte im Rahmen verschiedener unternehmensinterner Veränderungsprozesse mit der Beendigung seines Beschäftigungsverhältnisses rechnen müsse. Die Weiterbeschäftigung des Mitarbeiters sei gefährdet.

Hierzu wiesen wir darauf hin, dass die Bestellung der oder des behördlichen Datenschutzbeauftragten nur in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches, also nur aus wichtigem Grund, widerrufen werden könne. Wichtig seien ausschließlich Gründe, die mit der Funktion der oder des Beauftragten zusammenhängen und ihre weitere Ausführung unmöglich machten oder gefährdeten. Die ordentliche Kündigung des Arbeitsverhältnisses einer beziehungsweise eines behördlichen Datenschutzbeauftragten sei deshalb unzulässig. Die sich aus dem Arbeitsverhältnis ergebende Abhängigkeit der oder des Beauftragten dürfe sich nicht auf seine Funktion auswirken. Durch die Übertragung der Funktion der oder des behördlichen Datenschutzbeauftragten ergebe sich ein

besonderer Kündigungsschutz. Die mit der betont restriktiven Regelung des Widerrufsrechts angestrebte Absicherung der Unabhängigkeit der oder des Beauftragten dürfe nicht unterlaufen werden.

Der Betriebsrat des Unternehmens teilte uns auf unsere Stellungnahme mit, dass der behördliche Datenschutzbeauftragte am Ende weiterbeschäftigt und sein bis dahin befristeter Arbeitsvertrag entfristet wurde.

Wie an die Bestellung behördlicher Datenschutzbeauftragter nach dem Bremischen Datenschutzgesetz sind auch an die Beendigung dieser Funktion besondere gesetzliche Anforderungen gerichtet. Mit der Bestimmung, dass die Bestellung der oder des behördlichen Datenschutzbeauftragten von der verantwortlichen Stelle nur in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches, das heißt nur aus wichtigem Grund, widerrufen werden kann, wollte der Gesetzgeber der besonderen Bedeutung der Aufgabe der behördlichen Datenschutzbeauftragten Rechnung tragen. Eine solche Beendigung ist ausschließlich aus Gründen möglich, die mit der Funktion der Beauftragten zusammenhängen und die die weitere Ausübung dieser Funktion unmöglich machen oder gefährden. In der Kommentarliteratur werden als Beispiele hierfür schwerwiegende Versäumnisse bei der Beratung der verantwortlichen Stelle über die erforderlichen Datensicherheitsmaßnahmen, eine systematische Vernachlässigung der Prüfung einzelner Verarbeitungsbereiche, nachträglich festgestellte Mängel der Fachkunde, Verstöße gegen Verschwiegenheitspflichten und die beharrliche Weigerung, Beratungsverpflichtungen oder Schulungsverpflichtungen zu erfüllen, genannt.

Eine rechtmäßige Beendigung der Funktion der oder des behördlichen Datenschutzbeauftragten kann im gegenseitigen Einvernehmen oder durch Amtsniederlegung der oder des Beauftragten erfolgen. Voraussetzung dafür ist, dass die einvernehmliche Beendigung oder die Amtsniederlegung auf dem freien Willen der oder des Beauftragten beruhen.

Die dem Bremischen Datenschutzgesetz unterliegenden öffentlichen Stellen müssen auch die Beendigung des Amtes behördlicher Datenschutzbeauftragter unverzüglich der Landesbeauftragten für Datenschutz und Informationsfreiheit melden. In der Praxis unterbleibt diese Meldung demgegenüber häufig und wir erfahren erst durch die Meldung einer oder eines neuen behördlichen Datenschutzbeauftragten, dass die Vorgängerin oder der Vorgänger nicht mehr im Amt ist. Werden keine entsprechenden Gründe für die Beendigung der Amtsübertragung genannt, überprüfen wir bei der verantwortlichen Stelle die Berechtigung für diesen Schritt.

3.3 Workshops der behördlichen Datenschutzbeauftragten

Die Reihe der Workshops mit den behördlichen Datenschutzbeauftragten der Verwaltung wurde im Berichtsjahr fortgesetzt. Im Frühjahrsworkshop wurde schwerpunktmäßig das Thema „Sichere Kommunikation im und außerhalb des Bremer Verwaltungsnetzes“ behandelt. Bei der Kommunikation im und außerhalb des Bremer Verwaltungsnetzes sind besondere datenschutzrechtliche Anforderungen einzuhalten, um den Schutz personenbezogener Daten, die gerade im öffentlichen Bereich besonders sensibel sein können, zu gewährleisten. Geeignete und angemessene technische und organisatorische Maßnahmen sind zu ergreifen, die die ordnungsgemäße Anwendung der Verfahren sicherstellen. Zu den Aufgaben der behördlichen Datenschutzbeauftragten gehört es, die Einhaltung der ergriffenen Maßnahmen zu überwachen. Der angebotene Workshop stieß bei den behördlichen Datenschutzbeauftragten der bremischen Verwaltung auf große Resonanz, sodass er nach seiner erstmaligen Durchführung am gleichen Ort noch einmal wiederholt wurde.

In diesem Workshop wurde der Wunsch an uns herangetragen, die Treffen der behördlichen Datenschutzbeauftragten zu intensivieren und häufiger Veranstaltungen für die Beauftragten, die insbesondere auch dem gegenseitigen Erfahrungsaustausch dienen sollen, anzubieten. Daher luden wir im Herbst zu einem weiteren Treffen ein, an dem neben

den Datenschutzbeauftragten der bremischen Verwaltung auch die Beauftragten der Stadtverwaltung Bremerhaven teilnahmen. Die Veranstaltung diente primär dem gegenseitigen Austausch über die bei der Amtsausübung gesammelten Erfahrungen. Daneben nahmen wir zu der Frage Stellung, welche Daten in E-Mails enthalten sein dürfen und welche Anforderungen an eine Ende-zu-Ende-Verschlüsselung zu richten sind. Auch diese Veranstaltung stieß auf große Resonanz.

Die Datenschutzbeauftragten nutzten die Gelegenheit, über ihre Tätigkeit, ihre Erfahrungen und ihre Probleme bei der Amtswahrnehmung zu berichten und diese mit den anderen Teilnehmerinnen und Teilnehmern zu diskutieren. Als problematisch wurden insbesondere die den Beauftragten neben ihren sonstigen Tätigkeiten fehlende Zeit für die Wahrnehmung ihrer Aufgaben sowie die nicht rechtzeitige Unterrichtung über Vorhaben der automatisierten Verarbeitung personenbezogener Daten geschildert. Die Vertreter der Landesbeauftragten für Datenschutz und Informationsfreiheit boten den behördlichen Datenschutzbeauftragten an, sie, soweit es ihnen möglich ist, bei der Lösung der dargestellten Probleme zu unterstützen. Gleichzeitig äußerten die Datenschutzbeauftragten den Wunsch, ein solches Treffen in 2015 möglichst bald zu wiederholen.

4. Verwaltungsübergreifende Verfahren

4.1 BASIS.Bremen

Zur Umsetzung des Anforderungskatalogs der Landesbeauftragten für Datenschutz und Informationsfreiheit (vergleiche hierzu die neun Punkte unter Ziffer 4.4 im 36. Jahresbericht) wurde im Dezember 2013 von der Senatorin für Finanzen ein fortlaufender Workshop unter Beteiligung der Senatorin für Soziales, Kinder, Jugend und Frauen und dem Institut für Informationsmanagement Bremen GmbH (ifib) eingerichtet, an dem wir regelmäßig in beratender Funktion teilnahmen. In dem Bereich organisatorische und technische Grundlagen wurden die im Folgenden dargestellten Ergebnisse erzielt.

Um die Wahrnehmung der datenschutzrechtlichen Verantwortung durch die Dienststellen gewährleisten zu können, müssen die Kommunikationswege und die Verteilung der Aufgabenwahrnehmung zwischen der verantwortlichen Stelle, der Senatorin für Finanzen und Dataport als Dienstleister festgelegt werden. Hierzu entwarf die Senatorin für Finanzen eine Vereinbarung, die wir gegenwärtig gemeinsam abstimmen. Mit der Entwicklung eines allgemein verwendbaren Formblatts (Template), die zusammen mit Mitarbeiterinnen und Mitarbeitern aus dem Sozialressort anhand konkreter Geschäftsprozesse erfolgte, wurde eine erste Grundlage zur Ermittlung der für die Durchführung einer Strukturanalyse notwendigen Datenbasis geschaffen. Dieser Erhebungsbogen soll unter anderem die Grundlage für die Erstellung generischer Fachdatenschutzkonzepte bilden. Die für die Freie Hansestadt Bremen dokumentierte Umsetzung der Dienste Active Directory und Exchange wird erst bei der Überführung in das Rechenzentrum erfolgen. Im Rahmen von BASIS.Bremen wurden bereits einige übergreifende Prozesse definiert. Hiervon wird zuerst der Service zur zentralen Speicherung von Dateien (File-Service) bearbeitet. Des Weiteren wurde Dataport mit der Erstellung eines Verschlüsselungskonzeptes beauftragt. Im Oktober 2014 übergab Dataport der Senatorin für Finanzen eine Sicherheitsdokumentation für die Administrationsplattform. Zurzeit prüft die Senatorin für Finanzen, ob diese Dokumentation als Sicherheitsnachweis ausreicht.

Damit ergibt sich für uns das folgende Bild: Zwar sind die bisher erzielten Ergebnisse und formulierten Arbeitspakete ein sinnvoller Anfang. Da aber die Strukturanalyse noch nicht erfolgt ist und die darauf und auf die Schutzbedarfsfeststellungen aufbauende Risikoanalyse fehlt, ist noch keine Definition der für einen hohen und sehr hohen Schutzbedarf erforderlichen zusätzlichen Maßnahmen erfolgt und demzufolge auch kein Prozess für deren Beantragung etabliert. Deshalb sind die Voraussetzungen, nach denen die Dienststellen ihre nach dem Bremischen Datenschutzgesetz bestehende Verantwortung wahr-

nehmen können, noch nicht vorhanden. Es ist zu vermuten, dass für die Behebung der bestehenden Mängel noch ein erheblicher Zeitaufwand erforderlich sein wird. Der seit 2012 laufende Migrationsprozess wird damit ohne die vollständige Umsetzung der wesentlichen datenschutzrechtlichen Anforderungen abgeschlossen werden.

Besonders bedenklich ist diese Situation für Dienststellen, die besonders sensible Daten verarbeiten, die mindestens den Schutzbedarf hoch haben, und die Wahrung von Berufsgeheimnissen gemäß § 203 Absatz 1 Strafgesetzbuch sicherstellen müssen, wie zum Beispiel das Gesundheitsamt Bremen. Solche Dienststellen haben als datenschutzrechtlich verantwortliche Stellen die technischen und organisatorischen Maßnahmen zu treffen, die gewährleisten, dass externen Dienstleistern alle Möglichkeiten der Kenntnisnahme der Geheimnisse entzogen sind. Die folgenden Analysen müssen daher vor Beginn des Migrationsprozesses im Rahmen von BASIS.Bremen durchgeführt und die sich daraus gegebenenfalls ergebenden Maßnahmen umgesetzt worden sein.

Zur datenschutzgerechten Modellierung der Clients ist es erforderlich, eine Abgrenzung der Fachverfahren vorzunehmen. Wir halten eine parallele Betrachtung der Fachverfahren für erforderlich, wenn über die Clients auf Fachverfahren zugegriffen wird und im Rahmen des BASIS-PC Dokumente, die sensible Daten enthalten, bearbeitet werden. Inwieweit ein Risiko für die im Zusammenhang mit den Fachverfahren verarbeiteten Daten besteht, lässt sich erst anhand der Analyse konkreter Geschäftsprozesse bewerten. Der Schutzbedarf der Daten muss festgestellt und die Geschäftsprozesse in Bezug auf den PC-Einsatz analysiert werden. Die Netzstruktur des lokalen Netzes, die für den BASIS.Bremen Prozess relevanten Teile des Bremer Verwaltungsnetzes (BVN) und des Netzes des externen Dienstleisters sowie dessen administrative Zugriffe müssen ebenfalls analysiert sein, es muss eine revisionssichere Kontrolle der Fernzugriffe durch die externe Administration geben und die Kenntnisnahme sensibler Daten durch den externen Dienstleister verhindert werden. Die Authentizität der am Verfahren beteiligten Komponenten muss sichergestellt, die Risiken aufgrund der vorhandenen Datenbasis müssen ermittelt und konkrete Gegenmaßnahmen beauftragt sein. Das Gesundheitsamt haben wir darauf hingewiesen, dass es dem aktuellen Rahmendatenschutzkonzept BASIS.Bremen Version 1.0 (Ziffer 3.3) entspricht, alternativ zur Migration eigene Systeme für Verfahren mit hohen und sehr hohen Schutzbedarfen zu betreiben. Angesichts des aktuellen Umsetzungsstands der datenschutzrechtlichen Anforderungen halten wir die Vorhaltung eigener Systeme zumindest so lange für erforderlich, bis Dataport als externer Dienstleister den für die jeweilige Dienststelle erforderlichen Schutzbedarf sicher gewährleisten kann.

4.2 Sichere Administrationsumgebung bei Dataport

Über die Thematik der sicheren Administrationsumgebung bei Dataport haben wir bereits mehrfach berichtet (zuletzt im 36. Jahresbericht, Ziffer 4.3). Zwischenzeitlich erhielten wir Unterlagen, die unter anderem auch Aspekte der Administrationsplattform zur Verfahrensadministration bei Dataport enthalten. Wir befinden uns derzeit in einer kursorischen Durchsicht der Unterlagen. Eine Bewertung konnte noch nicht erfolgen.

Zur bremischen Administrationsplattform, die im Rahmen von BASIS.Bremen (siehe Ziffer 4.1 dieses Berichts) betrieben und durch zahlreiche zusätzliche Maßnahmen die Anforderungen eines hohen Schutzbedarfs erfüllen soll, teilte der Senat in seiner Stellungnahme zum 36. Jahresbericht mit, dass sich das Konzept in der Anpassung befinde und dass die Senatorin für Finanzen dem Auftragnehmer Dataport Ihre Anforderungen dazu übermittelt habe.

Wir gehen daher davon aus, dass uns diese Unterlagen und eine eigene Position der Senatorin für Finanzen zur bremischen Administrationsplattform und der von ihr genutzten Werkzeuge in Kürze vorgelegt werden. Sobald wir die Datenschutzdokumentation zur bremischen Administrationsplattform und eine Stellungnahme der Senatorin für Finanzen dazu vorliegen haben, werden wir die Unterlagen bewerten und dabei Schwerpunkte le-

gen auf die Gewährleistung des gesicherten Zugangs von Administratorinnen und Administratoren, die Beschränkung ihres Zugriffs auf berechtigte Verfahren, die Verschlüsselung auf dem Übertragungsweg, die Vollständigkeit und die Prüfbarkeit der Protokollierung sowie die Gewährleistung der Revisionsfähigkeit der Administrationsplattform.

4.3 Flächendeckende Einführung des Dokumentenmanagementsystems VISkompakt

Bereits mehrfach berichteten wir über die flächendeckende Einführung der elektronischen Akte mit dem Dokumentenmanagementsystem VISkompakt (zuletzt im 36. Jahresbericht, Ziffer 4.1).

In diesem Berichtsjahr übersandte uns die Senatorin für Finanzen das Datenschutzkonzept zu VISkompakt. Das Datenschutzkonzept stellt eine gute Basis dar, um darauf aufbauend den Gesamtumfang der zu treffenden Maßnahmen zu bestimmen und umzusetzen. Wir nahmen zu diesem Konzept umfassend Stellung und erörterten gemeinsam die noch zu klärenden Themen. Dazu gehört beispielweise die Abgrenzung zwischen zentralem Datenschutzkonzept der Senatorin für Finanzen zu VISkompakt und den dezentralen Datenschutzkonzepten einzelner Behörden und Dienststellen zu VISkompakt, die Regelungslücken verhindern soll. Außerdem besteht Klärungsbedarf beziehungsweise Ergänzungsbedarf bei der Protokollierung und dem zentralen Rechtekonzept und Rollenkonzept. Das angekündigte Konzept zum Löschen in VISkompakt liegt uns noch nicht vor. Zur Frage des Entzugs einer Berechtigung nach Bearbeitung einer Geschäftsgangsverfügung erhielten wir die Rückmeldung, dass diese Problematik mit einer zukünftigen Programmversion behoben sein wird. Wir würden sehr begrüßen, wenn auch für die Zwischenzeit eine Lösung gefunden würde.

Als strittiges Thema ist weiterhin die Umsetzung der Mandantenfähigkeit zu nennen. Die Senatorin für Finanzen sagte uns zu, dieses Thema gesondert zu prüfen, die vorgesehene Verfahrensgestaltung, beispielsweise zur Umsetzung der abgeschlossenen Datennutzungen, der Unabhängigkeit der Konfiguration sowie der ablagenübergreifenden und mandantenübergreifenden Berechtigungsvergabe zu beschreiben und mögliche Gefährdungen zu ermitteln. Diese Thematik ist von übergeordneter Bedeutung. Daher empfehlen wir eine bevorzugte Bearbeitung.

Zur Verschlüsselung von Daten mit hohem Schutzbedarf konkretisierten wir die datenschutzrechtlichen Anforderungen. Wir gehen davon aus, dass die Senatorin für Finanzen nun die Umsetzungsmöglichkeiten prüft. Wegen der Zugriffsregelung bei VISkompakt über Gruppen im Active Directory ist es möglich, dass absichtlich oder auch versehentlich durch Fehler in der Rechtevergabe Unberechtigte Zugriff auf Daten außerhalb ihrer eigentlichen Zugriffsberechtigung und Zuständigkeit erhalten können; sogar dienststellenübergreifend oder ressortübergreifend. Daher forderten wir, dass verantwortliche Stellen die Möglichkeit erhalten, eine zusätzliche Authentifizierungsmaßnahme bei Daten mit hohem Schutzbedarf zu beauftragen.

Wir begleiten darüber hinaus das Projekt „Elektronisierung von Sachakten“, dessen Ziel die Überführung von Sachakten in eine digitale Form ist. Hier gaben wir Hinweise zur Auftragsdatenverarbeitung, zu den Scanprozessen und zum Einsatz von Signaturen. Wir gehen davon aus, dass diese Themen im weiteren Verlauf des Projektes Berücksichtigung finden werden.

Außerdem erhielten wir im Berichtsjahr ein Fachkonzept zur Aussonderung, Vernichtung und Archivierung mit VISkompakt. Wir nahmen Stellung und erörterten unsere Anforderungen. Wir gehen davon aus, dass offene Fragen beispielsweise zur Revisionssicherheit sowie zur sicheren Übermittlung und sicheren Löschung von Daten in Kürze geklärt werden können.

Auch zur elektronischen Handakte nahmen wir gegenüber der Senatorin für Finanzen Stellung. Die elektronische Handakte bezeichnet eine Vorgehensweise, bei der elektronische Akten teilweise oder komplett exportiert und auf mobilen Endgeräten weiterverarbeitet werden. Wir forderten die Schaffung einer technischen Möglichkeit, den Export über Berechtigungen zu begrenzen und somit nur für bestimmte, klar definierte Bereiche zuzulassen. Der Export soll im Rahmen der Weitergabekontrolle nach dem Bremischen Datenschutzgesetz protokolliert werden. Die Nutzung der elektronische Handakte setzt voraus, dass die Weiterverarbeitung der Daten in einer Einsatzumgebung erfolgt, die dem festgestellten Schutzbedarf der Daten entspricht. Dafür sind geeignete Nutzungskonzepte, Sicherheitskonzepte und Datenschutzkonzepte notwendig, die vor einer Nutzung mit Echtdaten vorliegen und umgesetzt sein müssen. Darin sollen neben der Festlegung der technischen und organisatorischen Maßnahmen zur Gewährleistung der Vertraulichkeit auch Fragestellungen zur Gewährleistung des Auskunftsrechts über gespeicherte Daten sowie der Verpflichtung zur sicheren Löschung der Daten behandelt werden.

Wir begrüßen die Aussage der Senatorin für Finanzen im Datenschutzkonzept, das Verfahren VISkompakt bezüglich des Betriebs im Rechenzentrum und der Aspekte „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ mit dem Schutzbedarf „hoch“ zu beauftragen. Die Maßnahmenfestsetzung und Realisierung von verfahrensspezifischen Maßnahmen, wie etwa die erwähnte Verschlüsselung und eine zusätzliche Authentifizierung bei hohem Schutzbedarf, steht noch aus. Das Verfahren VISkompakt hat darüber hinaus bezüglich der Berechtigungsvergabe Bezüge zum Active Directory, zur Administrationsplattform (siehe Ziffer 4.2 dieses Berichts) sowie zu BASIS.Bremen (siehe Ziffer 4.1 dieses Berichts). Nur durch das richtige Zusammenwirken aller Komponenten kann die Gesamtsicherheit hergestellt werden.

Für die noch offenen Punkte hat die Senatorin für Finanzen einen Zeitplan angekündigt, dessen Umsetzung wir begleiten werden.

4.4 Anforderungen an den Betrieb von SAP

Bereits in den vergangenen Berichtsjahren berichteten wir mehrfach (vergleiche 36. Jahresbericht, Ziffer 4.2; 34. Jahresbericht, Ziffer 4.3; 33. Jahresbericht, Ziffer 4.1 und 32. Jahresbericht, Ziffer 10.3) über die Anforderungen an den Datenschutz bei dem Verfahren SAP.

Zum Projekt der Reorganisation der Berechtigungen hatten wir im vergangenen Berichtsjahr die Erstellung einer anonymisierten beziehungsweise pseudonymisierten Datenbasis für den Integrationstest gefordert. Zumindest erwarteten wir ein spezielles Sicherheitskonzept, aus dem hervorgeht, wie der unberechtigte Zugriff in dieser Projektphase verhindert wird. Zwar teilte der Senat in seiner Stellungnahme zum 36. Jahresbericht mit, dass die Datensicherheit über besondere Einstellungen in den Berechtigungen gesichert sein würde, ein Konzept dafür erhielten wir allerdings bislang nicht. Eine Rückmeldung der Senatorin für Finanzen des Inhalts, dass die Umsetzung von Maßnahmen aus dem Berechtigungskonzept vollständig erfolgt sei, liegt uns ebenfalls nicht vor. Außerdem erhielten wir keine Rückmeldung zur Realisierung der speziellen Berechtigungen für Kreditorenstämme im SAP-Verfahren (vergleiche Ziffer 10.1 dieses Berichts).

Unsere Forderung nach einer Anonymisierung beziehungsweise Pseudonymisierung der Datenbasis wird in gleicher Stellungnahme des Senats als nachvollziehbar angesehen. Ab Mitte dieses Berichtsjahres sollte daher die Einführung eines geeigneten SAP-Tools für diese Zwecke geprüft werden. Wir begrüßen diese Ankündigung und gehen davon aus, dass uns nun in Kürze das Ergebnis der Prüfung vorgelegt werden kann.

Bezüglich der Nutzung besonderer Systemkomponenten von SAP beispielsweise zur Steuerung und Konvertierung von Daten zwischen zwei Systemen (vergleiche Ziffer 4.5 dieses Berichts), forderten wir die Einhaltung des Trennungsgebotes und fragten bei der Se-

natorin für Finanzen an, ob weitere spezielle Systemkomponenten möglicherweise länderübergreifend genutzt werden. Auch dazu steht eine Antwort noch aus.

Zum Ticketmanagement erhielten wir erneut umfangreiche Unterlagen. Zum Berechtigungskonzept und seinen Anlagen nahmen wir nochmals Stellung. Diesbezüglich sehen wir Ergänzungs-, Erklärungs- sowie Vervollständigungsbedarf. Zu unseren Hinweisen zum geplanten Verfahren der Zurücksetzung von Kennwörtern erwarten wir erneut nähere Angaben, da die bisherigen Angaben nach unserer Auffassung noch unvollständig sind. Die Verfahrensbeschreibung und das Datenschutzkonzept befinden sich in erneuter Durchsicht. Wir werden diesbezüglich Kontakt mit der fachlichen Leitstelle SAP aufnehmen.

Nach wie vor erwarten wir den Beginn der angekündigten Folgeprojekte zu einer kontinuierlichen Anpassung der Dokumentenlage und deren Umsetzung. Gemäß § 7 Absatz 2 Bremisches Datenschutzgesetz sind die Datenschutzdokumentationen laufend auf dem neuesten Stand zu halten. Es ist wichtig, dass die fachliche Leitstelle ausreichende personelle Ressourcen zur Verfügung hat, um die umfassenden Aufgaben in diesem Bereich bewältigen zu können.

4.5 Elektronischer Einkaufskatalog BreKAT

In diesem Berichtsjahr begleiteten wir die Einführung des neuen elektronischen Katalogsystems und Bestellsystems BreKAT. Über diese elektronische Plattform können öffentliche Stellen und Stellen, an denen die Freie Hansestadt Bremen beteiligt ist, Waren und Dienstleistungen einkaufen, zu denen im Vorfeld Rahmenverträge abgeschlossen wurden.

Wir nahmen zu dem Rahmendatenschutzkonzept und dem technischen Konzept Stellung und legten unsere Anforderungen an einen datenschutzkonformen Einsatz des BreKAT dar. Wir hatten hinsichtlich der Infrastruktur Bedenken. Unsere daraus resultierenden Anforderungen wurden umgesetzt. Im Projekt ist geplant, eine Schnittstelle zwischen dem Verfahren BreKAT und dem Verfahren SAP zur automatisierten Übertragung von Bestelldaten einzurichten. Bezüglich dieser Schnittstelle erwarten wir unter anderem die Darlegung von Maßnahmen zur Gewährleistung des Trennungsgebotes sowie die Umsetzung existierender Leitlinien des Herstellers für die eingesetzten Komponenten. Wir gehen davon aus, dass uns durch die verantwortliche Stelle eine geeignete Dokumentation zur Schnittstelle selbst, den damit verbundenen Kundeneinstellungen, dem Authentifizierungsverfahren sowie der erforderlichen Berechtigungen im SAP rechtzeitig vor Produktivstart der Schnittstelle vorgelegt wird.

5. Inneres und Sport

5.1 Mikrozensus

Immer wieder erreichen uns Anfragen zum Mikrozensus. Es handelt sich dabei um eine repräsentative Haushaltsbefragung zur Bevölkerungsstruktur sowie zur wirtschaftlichen und sozialen Lage der Bevölkerung. Nach einem festgelegten Zufallsverfahren wird dafür eine bestimmte Prozentzahl von Wohnungen ausgewählt, deren Bewohnerinnen und Bewohner viermal im Abstand von etwa einem Jahr Fragen zu Themen wie beispielsweise Familie, Erwerbstätigkeit, Ausbildung, Wohnsituation und Gesundheit beantworten müssen. Die Fragen können entweder schriftlich oder in einem persönlichen Gespräch gegenüber den Interviewerinnen und Interviewern der Statistischen Landesämter beantwortet werden. Die daraus erstellten Statistiken richten sich in erster Linie an die Verantwortlichen aus Parlamenten, Verwaltung und Wissenschaft, aber auch an die Öffentlichkeit.

Häufig werden wir gefragt, ob die Angaben, die sehr viele Informationen über die Befragten preisgeben, verpflichtend oder freiwillig sind. Wir teilen den Betroffenen dann mit, dass grundsätzlich eine Auskunftspflicht besteht, von der keine Befreiungen vorgesehen sind.

Lediglich bestimmte Zusatzfragen sind freiwillig. Geregelt ist dies im Mikrozensusgesetz und Bundesstatistikgesetz.

Oft befürchten die Betroffenen, dass ihre Daten weitergegeben und von anderen Behörden abgeglichen würden. Es gilt jedoch der Grundsatz, wonach die Angaben ausschließlich für statistische Zwecke verwendet werden dürfen und strikt geheim zu halten sind. Die persönlichen Angaben der Befragten wie Name und Anschrift, sogenannte Hilfsmerkmale, werden von den restlichen Angaben getrennt gespeichert und nach Abschluss der Aufbereitung der Befragung vernichtet.

Eine Petentin teilte uns mit, dass sich bei ihr ein Erhebungsbeauftragter zur Durchführung des Mikrozensus angemeldet hätte. Die Befragung sollte mit Hilfe eines Laptops oder der Erhebungsbögen durchgeführt werden. Der Interviewer habe dann aber Informationen auf einem Notizblock festgehalten, was der Petentin merkwürdig vorkam. Wir baten daraufhin das Statistische Landesamt um Stellungnahme. Dies teilte uns mit, dass der betroffene Mitarbeiter zum Sachverhalt befragt worden sei. Dabei stellte sich heraus, dass er sich im Umgang mit dem Laptop unsicher gefühlt und deshalb die Antworten zunächst auf einem Papierbogen aufgeschrieben habe. Zuhause habe er die Daten dann in Ruhe in den Computer eingegeben und die schriftlichen Unterlagen vernichtet. Die Nutzung der Fragebögen sei von ihm als sehr zeitaufwendig empfunden worden. Das Statistische Landesamt habe dem Interviewer daraufhin erläutert, dass seine Vorgehensweise nicht den gesetzlichen Anforderungen entspreche und ihn angewiesen, ab sofort ausschließlich das Laptop oder die amtlichen Mikrozensusfragebögen zu verwenden. Wir gehen davon aus, dass die gesetzlichen Vorgaben nunmehr eingehalten werden.

5.2 Telekommunikationsüberwachung durch die Polizeien

Seit geraumer Zeit kooperieren nun die Polizeien Bremen und Bremerhaven bei der Telekommunikationsüberwachung mit dem Landeskriminalamt Niedersachsen. Zur eingereichten Dokumentation hatten wir bereits in den vergangenen Berichtsjahren (vergleiche 36. Jahresbericht, Ziffer 5.1 und 35. Jahresbericht, Ziffer 5.11) umfassend Stellung genommen und unsere Anforderungen daran dargelegt. In der vorliegenden Stellungnahme des Senats zum 36. Jahresbericht wurden die Gründe für die Verzögerung bei der Vorlage von aktualisierten Unterlagen benannt. Die nun für das Ende dieses Berichtsjahres angekündigten Unterlagen sind allerdings bislang nicht bei uns eingegangen. Weiterhin ist unklar, ob die von uns eingebrachten Vorschläge zur Änderung und Ergänzung des Verwaltungsabkommens Eingang in die unterschriftsfähigen Unterlagen gefunden haben.

5.3 Allgemeines zu den Polizeiverfahren

Verschiedene Polizeiverfahren sind seit längerem Gegenstand unserer datenschutzrechtlichen Beratung der Polizei Bremen. Zum Vorgangsbearbeitungssystem @rtus (vergleiche 36. Jahresbericht, Ziffer 5.5) erhielten wir im Berichtsjahr ergänzende Angaben, die wir derzeit bewerten. Im Vergleich zum Vorjahr hat sich allerdings in den folgenden Themengebieten nichts Wesentliches geändert: Zum Fachverfahren INPOL-Land (vergleiche 36. Jahresbericht, Ziffer 5.4), dem Rahmendatenschutzkonzept der Polizei Bremen (vergleiche 36. Jahresbericht, Ziffer 5.8), wie beispielsweise aber auch zum Intensivtäterkonzept des Handlungskonzepts „Stopp der Jugendgewalt“, dem internen Portal der Polizei Bremen (Intrapol), dem Fachverfahren zur Einsatzleitzentrale oder etwa dem digitalen Sprechfunk und Datenfunk der Behörden und Organisationen mit Sicherheitsaufgaben sind keine neuen Unterlagen bei uns eingegangen. Gleiches gilt auch für unsere Fragestellungen zur Telekommunikationsüberwachung (siehe Ziffer 5.2 dieses Berichts). Somit besteht weiterhin dringender Handlungsbedarf aufseiten der Polizei Bremen, um uns bei unserer gesetzlichen Aufgabenerfüllung zu unterstützen.

Dies wurde auch auf der Sitzung des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit der Bremischen Bürgerschaft zum 36. Jahresbericht am

24. Oktober 2014 erörtert (siehe Drucksache der Bremischen Bürgerschaft 18/1690 vom 17. Dezember 2014, Ziffer 2.1 dieses Berichts). Vom Ausschuss wurden die zum Teil erheblichen Defizite bei der Umsetzung der datenschutzrechtlichen Anforderungen, die an die Polizei Bremen gestellt werden, kritisiert. Der Ausschuss stellte ferner fest, dass der Verweis auf fehlendes Personal nicht dazu führen dürfe, dass den datenschutzrechtlichen Anforderungen als gesetzlichen Verpflichtungen durch öffentliche Stellen nicht nachgekommen werde. Der Ausschuss bekräftigte, dass die Erledigung der mit den datenschutzrechtlichen Anforderungen verbundenen Aufgaben durch die Polizei Bremen sichergestellt werden müsse.

5.4 Data Center Polizeien

In diesem Berichtsjahr führten wir mit dem Senator für Inneres und Sport, Dataport, Vertretern der anderen Landesbeauftragten für den Datenschutz und den betroffenen Länderpolizeien diverse Gespräche zu dem Thema Auftragsdatenverarbeitung für die Polizeien Schleswig-Holstein, Hamburg und Bremen bei Dataport (kurz genannt „Data Center Polizeien“). Vor dem Hintergrund der Sicherheitsrelevanz der durch die Länderpolizeien verarbeiteten personenbezogenen Daten und genutzten Verfahren und deren vorgesehener Kumulation bei der Anstalt des öffentlichen Rechts Dataport als Auftragnehmerin formulierten wir datenschutzrechtliche Anforderungen an die Datensicherheit und an die Trennung der polizeilichen Datenverarbeitung zwischen den verschiedenen Ländern, welche das Trennungsgebot gewährleisten sollen. Das Trennungsgebot folgt aus § 7 Absatz 4 Satz 2 Nummer 8 Bremisches Datenschutzgesetz und formuliert die Anforderung, dass zu gewährleisten ist, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Wir forderten insbesondere, dass auch im Data Center Polizeien die personenbezogenen Daten der jeweiligen Länderpolizeien gegeneinander abgeschottet sind.

Zwar ist ein länderübergreifender Datenaustausch unter Beachtung der jeweiligen Datenübermittlungsvorschriften und Datenerhebungsvorschriften derzeit nicht geplant. In die Betrachtungen müssen aber nicht nur geplante, rechtlich abgesicherte, sondern auch ungeplante, aber technisch mögliche Zugriffsmöglichkeiten einbezogen werden. Weiterhin wiesen wir auf die datenschutzrechtlichen Vorgaben für automatisierte Abrufe polizeilicher personenbezogener Daten aus anderen Bundesländern und für gemeinsame polizeiliche Verfahren, die eine Rechtsgrundlage fordern, hin.

5.5 Einsatzleitzentrale der Ortspolizeibehörde Bremerhaven

In diesem Berichtsjahr ließen wir uns nach Vorlage der Verfahrensbeschreibung das Fachverfahren der Einsatzleitzentrale der Ortspolizeibehörde Bremerhaven vor Ort zeigen und übermittelten im Anschluss daran unsere Hinweise zur Verbesserung des Datenschutzes. Eine Einsichtnahme in die Protokolldaten war zu diesem Zeitpunkt nicht möglich. Wir baten daher den behördlichen Datenschutzbeauftragten der Ortspolizeibehörde Bremerhaven, die Protokollierung auf Gewährleistung der Eingabekontrolle nach § 7 Bremisches Datenschutzgesetz zu prüfen. Das Ergebnis seiner Prüfung liegt uns bislang nicht vor. Weiterhin nahmen wir Stellung zur geänderten Verfahrensbeschreibung zum Fachverfahren der Einsatzleitzentrale. Diese Dokumentation verweist bezüglich der technischen und organisatorischen Maßnahmen in einigen Punkten auf das Rahmendatenschutzkonzept der Ortspolizeibehörde Bremerhaven, sodass wir darum baten, uns das aktuelle Konzept zukommen zu lassen. Erst dann kann eine abschließende und vollständige Bewertung unsererseits erfolgen.

5.6 Auskunftsbegehren und Löschbegehren von Bürgerinnen und Bürgern gegenüber der Polizei Bremen

Bürgerinnen und Bürger sprechen uns an, wenn sie mit der Auskunft der Polizei Bremen unzufrieden sind, weil zum Beispiel das staatsanwaltschaftliche Aktenzeichen oder auch

der Verfahrensausgang in der polizeilichen Auskunft nicht vermerkt sind, oder sie Speicherungen für unzulässig halten und gelöscht haben wollen. Im letzteren Fall überprüfen wir die Zulässigkeit der polizeilichen Speicherungen und kamen in diesem Berichtsjahr in einem von fünf Fällen dazu, dass alle der 18 Speicherungen als Tatverdächtiger wegen Unzulässigkeit der Speicherung zu löschen waren. Unter anderem wurden zu dem Bürger – mehrfach aufgrund von Nachbarschaftsstreitigkeiten – folgende Verdachtsfälle gespeichert: Nachstellung gemäß § 238 Strafgesetzbuch, einige Körperverletzungen gemäß § 223 und § 224 Strafgesetzbuch, mehrere Beleidigungen gemäß § 185 Strafgesetzbuch, einige Diebstähle gemäß § 242 Strafgesetzbuch, falsche Verdächtigung gemäß § 164 Strafgesetzbuch und Hausfriedensbruch gemäß § 123 Strafgesetzbuch. Der älteste Eintrag war unerlaubtes Entfernen vom Unfallort gemäß § 142 Strafgesetzbuch und stammte aus dem Jahr 2002, während die jüngste Speicherung in 2013 vorgenommen wurde. Alle Ermittlungsverfahren in diesen Verdachtsfällen wurden durch die Staatsanwaltschaft eingestellt. Dieser Fall aus unserer Praxis ist beispielhaft dafür, wo wir unzulässige Speicherungen aufspüren und Löschungen erreichen konnten.

Außerdem ist es uns ein Anliegen, dass der Verfahrensausgang durch die Staatsanwaltschaft der Polizei gemäß der Strafprozessordnung zeitnah mitgeteilt wird. Dies ist wichtig, da die Speicherfristen maßgeblich durch den Verfahrensausgang bestimmt werden und nur überprüfbar sind, wenn diese Information vorliegt. Ist der Verfahrensausgang unbekannt, erfragen die Polizeien erst anlässlich eines Auskunftsersuchens einer Person diesen Verfahrensausgang bei der Staatsanwaltschaft. Erst dann wird die polizeiliche Speicherung durch die Polizei selbst überprüft. Wir begrüßen es, dass dieser Kommunikationsweg zwischen Staatsanwaltschaft und Polizei aufgrund einer Schnittstelle im neuen Vorgangsbearbeitungssystem der Polizeien zu dem Vorgangsbearbeitungssystem der Staatsanwaltschaft verbessert wurde.

5.7 Antiterrordatei

Auf der Grundlage des Antiterrordateigesetzes vom 22. Dezember 2006 wird von verschiedenen Sicherheitsbehörden eine gemeinsame standardisierte zentrale Antiterrordatei betrieben. Nach dem Antiterrordateigesetz obliegt die Kontrolle dieser Datei unter anderem der Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen. Mit Urteil vom 24. April 2013 hat das Bundesverfassungsgericht den schwachen Individualrechtsschutz bei heimlichen Dateien hervorgehoben, der durch die objektiv-rechtliche Kontrolle durch unabhängige Datenschutzbeauftragte kompensiert wird. Unter anderem hat es klargestellt, dass diese aufsichtsrechtliche Kontrolle regelmäßig und in angemessenen Abständen, etwa alle zwei Jahre, durchzuführen ist. Das Bundesverfassungsgericht stellt in seinem Urteil sowohl an die Legislative als auch an die Exekutive Anforderungen: In den Grundstrukturen als bloße Hinweisdatei, die eine Rasterung, Sammelabfragen oder die übergreifende Ermittlung von Zusammenhängen bisher nicht erlaube, wird die Antiterrordatei und das sie errichtende Gesetz für verfassungsgemäß gehalten, in der Ausgestaltung einzelner Punkte erfüllt das Antiterrordateigesetz nicht den verfassungsrechtlichen Anspruch. Ähnliche Regelungen existieren auch im Rechtsextremismus-Datei-Gesetz, sodass sich damit auch hier Änderungsbedarf ergibt. Im Berichtsjahr wurde an einer Änderung des Antiterrordateigesetzes gearbeitet, die diese judikativen Vorgaben mit Wirkung vom 1. Januar 2015 umsetzen soll. Insbesondere wurde seitens der Datenschützer zum Änderungsgesetzesvorschlag ins Feld geführt, dass hinsichtlich des Gewaltbegriffs nur das willentliche Hervorrufen von Gewalt eine Speicherung in der Antiterrordatei rechtfertigt, und dass die Legaldefinition von Kontaktperson als mit dem Bestimmtheitsgebot unvereinbar ist, gerade auch unter dem Aspekt der Definition der Verfassungsschutzbehörden und einer engeren Definition der Polizeibehörden. Bei einer Kontrolle müssen die Protokolldaten den Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen. Weiter wurden die damit einhergehenden Änderungen des Bundesverfassungsschutzgesetzes, des Bundeskriminalamtsgesetzes und des Bundesnachrichtendienstgesetzes zum Thema Projektdateien in Hinsicht auf das Gebot

der informationellen Trennung kritisiert. Als Konsequenz des Urteils des Bundesverfassungsgerichts und damit zur Erfüllung unserer Kontrollaufgabe haben wir im Berichtsjahr unsere Prüfung dieser stark umstrittenen Datei begonnen.

5.8 Erweiterte Führungszeugnisse in Sportvereinen

Ein Bremer Sportverein fragte uns, ob er das Ergebnis der Vorlage des erweiterten Führungszeugnisses, welches dem Bundessportverband bereits vorgelegt worden war, übermittelt bekommen dürfe. Der Hintergrund für diese Anfrage besteht darin, dass Sportvereine, die eine Übungsleiterin oder einen Übungsleiter engagieren möchten, nach dem Bundeszentralregistergesetz vor Abschluss des Trainervertrages zum Schutz von minderjährigen Sportlerinnen und Sportlern das erweiterte Führungszeugnis (umgangssprachlich auch polizeiliches Führungszeugnis genannt) von Übungsleiterinnen und Übungsleitern verlangen können. Es obliegt in einem solchen Fall der Übungsleiterin oder dem Übungsleiter zu entscheiden, ob sie oder er das erweiterte Führungszeugnis beantragen und dem Sportverein vorlegen möchte. Sofern sie sich dagegen entscheiden, müssen die Betreffenden damit rechnen, dass der Trainervertrag nicht zustande kommt (zum Umgang mit dem erweiterten Führungszeugnis innerhalb des Sportvereins siehe 34. Jahresbericht, Ziffer 5.13).

Bei der Beantwortung der datenschutzrechtlichen Frage muss zwischen Vereinen, die nach dem Sozialgesetzbuch (SGB) VIII zu behandeln sind, und Vereinen, die nicht gefördert werden und keine freien Träger der Jugendhilfe sind, unterschieden werden. Bei den erstgenannten Vereinen ist ein direkter Datenaustausch zwischen Sportvereinen beziehungsweise zwischen Vereinen und Verbänden datenschutzrechtlich unzulässig. Bei den nicht dem SGB VIII unterfallenden Vereinen kann die Übermittlung der Ergebnisses der Vorlage von Führungszeugnissen zwischen Sportvereinen nach dem Bundesdatenschutzgesetz zulässig sein.

Bei einer solchen Datenübermittlung muss geprüft werden, ob Grund zu der Annahme besteht, dass Ausschlussgründe wegen schutzwürdigem Interesse der betroffenen Übungsleiterin oder des betroffenen Übungsleiters bestehen. Hierfür ist entscheidend, dass nach dem Bundeszentralregistergesetz eine Übungsleiterin oder ein Übungsleiter selbst über die Vorlage ihres oder seines Führungszeugnisses zum Erwerb der Trainerlizenz entscheiden darf. Dieser Weg kann der Trainerin oder dem Trainer als betroffene Person genommen sein, wenn die Datenübermittlung direkt zwischen den Vereinen erfolgt. Solange zwischen den Verbänden und den Vereinen lediglich der Hinweis „Es bestehen keine Bedenken“ als Ergebnis der Vorlage des erweiterten Führungszeugnisses übermittelt wird, kann kein Ausschlussgrund angenommen werden und diese Information darf erforderlichenfalls zusammen mit der Information, wann die Auskunft aus dem Bundeszentralregister erteilt wurde, übermittelt werden. Auch die Tatsache, dass die Übungsleiterin oder der Übungsleiter bereits eine Trainerlizenz besitzt, ist ein Indiz dafür, dass keine Bedenken gegen diese Person aus Minderjährigenschutzgründen bestehen und darf deshalb übermittelt werden. In den Fällen, in denen keine Informationen über die angefragte Person vorhanden sind, und zur Vermeidung der expliziten Weitergabe einer negativen Auskunft sollte der anfragende Sportverein aufgefordert werden, selbst eine Einsicht in das Führungszeugnis zu verlangen und vorzunehmen. Die betroffene Übungsleiterin oder der betroffene Übungsleiter hat dann die Möglichkeit zu reagieren und ein erweitertes Führungszeugnis zu beantragen und vorzulegen. Diese Vorgehensweise trägt dem Umstand Rechnung, dass eine negative Information des Bundessportverbands veraltet sein kann. Eine aktuelle Einsichtnahme durch den anfragenden Sportverein kann die Angelegenheit klären. Außerdem können die betroffenen Übungsleiterinnen und Übungsleiter in diesem Fall selbst entscheiden, ob sie eine negative Eintragung offenbaren möchten oder die Offenbarung vermeiden und ihre Bewerbungen zurückziehen möchten. Das gleiche gilt für den Fall, dass keine Informationen über die angefragte Trainerin oder den angefragten Trainer beim Bundessportverband vorliegen und damit überhaupt keine Aussage des Bun-

dessportverbandes getroffen werden kann. Dieser Fall ist in der Vorgehensweise und Information dem Fall der Vermeidung einer negativen Auskunft gleichzustellen, damit keine Wertungen durch den anfragenden Verein vorgenommen und die betroffene Übungsleiterin oder der betroffene Übungsleiter nicht stigmatisiert werden können. Eine solche Vorgehensweise trägt dem schutzwürdigen Interesse der betroffenen Personen Rechnung. Wir empfehlen darüber hinaus eine Aufklärung der betroffenen Personen über das oben geschilderte Vorgehen und damit die Information über die direkte Datenübermittlung zwischen den Sportvereinen.

6. Gesundheit

6.1 Aufbau eines klinisch-epidemiologischen Krebsregisters in Bremen

Seit dem 1. Januar 1998 gibt es in Bremen ein epidemiologisches Krebsregister. Darin finden sich Informationen über einschlägig erkrankte Patientinnen und Patienten im Land Bremen. Mit Inkrafttreten des Krebsfrüherkennungs- und Krebsregistergesetzes im April 2013 wurden die Länder verpflichtet, klinische Krebsregister einzurichten. Die Aufgaben klinischer Krebsregister und die Rahmenbedingungen für ihre Finanzierung wurden dabei bundesgesetzlich bestimmt. Die Umsetzung der bundesgesetzlichen Vorgaben einschließlich der Regelungen zum Datenschutz soll durch Landesgesetze erfolgen.

Der Senator für Gesundheit wandte sich im Dezember 2013 an uns, um uns bereits frühzeitig in die Überlegungen zur Erarbeitung eines Entwurfs für ein entsprechendes Landesgesetz einzubeziehen. Vorgesehen war, das bisherige epidemiologische Krebsregister, welches im Wesentlichen Zwecken der Beobachtung und Erforschung von Krebserkrankungen diente, auf ein zukünftig kombiniertes klinisch-epidemiologisches Krebsregister, durch welches auch die Behandlung des jeweils Betroffenen unterstützt werden kann, zu erweitern.

Ende April 2014 erhielten wir den ersten Gesetzentwurf noch vor dem offiziellen Beteiligungsverfahren, sodass wir die Gelegenheit hatten, viele unserer Kritikpunkte bereits frühzeitig mit dem Senator für Gesundheit zu erörtern. Einige Verbesserungen konnten dadurch erreicht werden. Mitte August 2014 wurde uns dann ein überarbeiteter Entwurf im Rahmen des offiziellen Beteiligungsverfahrens zur Stellungnahme übersandt.

Bei dem Bremer Krebsregister auf der Grundlage des vorliegenden Gesetzentwurfs handelt es sich um eine Einrichtung, die die Erhebung, Verarbeitung und Nutzung von Daten über Krebserkrankungen namentlich benannter Personen und damit hochsensibler Gesundheitsdaten von den Betroffenen erzwingt. Da an diesen personenbezogenen Daten eine hohe Begehrlichkeit insbesondere aus dem Bereich der Forschung und der Pharmaindustrie besteht, sollten besonders hohe Schutzmaßnahmen getroffen werden, um das Risiko des potenziellen Missbrauchs der Daten so weit wie möglich zu minimieren.

Datenschutzrechtlich problematisch waren im vorliegenden Gesetzentwurf insbesondere die folgenden Aspekte:

Es ist keine räumliche, organisatorische und personelle Trennung der Vertrauensstelle, die die Identitätsdaten der Betroffenen speichert, und der Auswertungsstelle, die im Wesentlichen die medizinischen Daten unter einem Pseudonym speichert, vorgesehen. Stattdessen soll eine gemeinsame Leitung der beiden Stellen bestehen. Damit findet keine hinreichend klare Trennung von Auswertungsstelle und Vertrauensstelle statt. So wird ein erhöhtes Missbrauchsrisiko in Kauf genommen.

Zudem sollte unserer Auffassung nach die öffentliche Trägerschaft des Bremer Krebsregisters gesetzlich festgeschrieben werden. Insbesondere die Trägerschaft durch eine Forschungseinrichtung, die ein eigenes Interesse an den im Krebsregister gespeicherten Daten hat, birgt ein Missbrauchsrisiko. Dies betrifft insbesondere die Vertrauensstelle, in

der zukünftig nicht lediglich die Identitätsdaten, sondern auch die medizinischen Daten dauerhaft gespeichert werden sollen. Unseren Informationen nach ist es zwar offenbar gelungen, weiterhin die Kassenärztliche Vereinigung Bremen als Trägerin für die Vertrauensstelle zu gewinnen. Die neue gesetzliche Regelung erlaubt jedoch im Gegensatz zu den Gesetzen in Hamburg und dem Saarland auch eine private Trägerschaft der Vertrauensstelle.

Dringenden Änderungsbedarf sehen wir im Hinblick auf die im aktuellen Gesetzentwurf als „Widerspruchsrecht“ bezeichneten Regelungen. Die Formulierung „Widerspruchsrecht“ suggeriert, dass die Betroffenen die Möglichkeit haben, der Verarbeitung ihrer personenbezogenen Daten durch das Krebsregister zu widersprechen. Demgegenüber hat der „Widerspruch“ der Betroffenen nach der geplanten Regelung auf die Meldung durch die meldepflichtige Einrichtung keine Auswirkungen: Es wird genau der gleiche Datensatz gemeldet wie beim Verzicht auf einen sogenannten Widerspruch. Folge des sogenannten Widerspruchs ist lediglich, dass nach Abschluss der Abrechnungsverfahren und Erstattungsverfahren die Identitätsdaten der Betroffenen in der Vertrauensstelle pseudonymisiert werden. Wir sind der Auffassung, dass im Falle des Widerspruchs einer beziehungsweise eines Betroffenen gegen eine Speicherung im Krebsregister das Geheimhaltungsinteresse der oder des Betroffenen aufgrund der besonderen Sensibilität der Daten und der mit einer Krebserkrankung verbundenen erheblichen Belastungen wesentlich höher wiegt als das Interesse an einer vollständigen (nahezu hundertprozentigen) Erfassung der Krebserkrankungen zum Zweck der Durchführung der gesetzlich festgelegten Auswertungen und wissenschaftlicher Untersuchungen. Deshalb setzten wir uns für die Einführung eines echten gestuften Widerspruchsrechts der Betroffenen wie im Hamburger Gesetz ein, das ihnen die Möglichkeit gibt, entweder der gesamten Meldung durch die Ärztin beziehungsweise durch den Arzt oder lediglich der dauerhaften Speicherung der Identitätsdaten in der Vertrauensstelle rechtswirksam zu widersprechen. Zudem halten wir es für erforderlich, dass, wie in Hamburg, eine Regelung zur Ausübung des Widerspruchsrechts bei einwilligungsunfähigen Personen getroffen wird, und dass für die Betroffenen eine Möglichkeit zum Widerspruch gegen die Verarbeitung und Nutzung ihrer Daten zu Forschungszwecken nach § 16 Absatz 1 geschaffen wird. Diese Anforderungen sind bislang nicht ins Gesetz übernommen worden.

In Bezug auf das Auskunftsrecht der Betroffenen forderten wir, dass dieses im Umfang dem allgemeinen Auskunftsrecht im Bremischen Datenschutzgesetz entspricht. Die Regelung im aktuellen Gesetzentwurf bleibt deutlich dahinter zurück.

Ferner sahen wir erheblichen Überarbeitungsbedarf im Hinblick auf die Qualität des Pseudonymisierungsverfahrens. Für die Pseudonymisierung der Datensätze ist ein Verfahren vorgesehen, mit dem nicht alle Identitätsdaten pseudonymisiert werden sollen. Die Adresse soll durch die Ortsteilkennziffer oder sogar durch Gauß-Krüger-Koordinaten ersetzt werden. Mit einem solchen Verfahren sind die Mindestanforderungen an Pseudonymisierungen, wonach ein kryptografisches Verfahren verwendet werden muss, das einen irreversiblen Ausgangswert ergibt, nicht erfüllt. Gelöscht oder pseudonymisiert werden müssen alle Identitätsdaten, also auch Name und Anschrift des Trägers der Krankenversicherung sowie die Krankenversichertennummer oder ein vergleichbares Merkmal. Unbedingt sollte auf die Verwendung von sprechenden Sortierkriterien, sogenannten Ordnungsmerkmalen als Kennziffer für die Pseudonymisierung verzichtet werden. Die für ein Pseudonymisierungsverfahren verwendete Kennziffer darf selbst keine eigene Information enthalten. Das Verfahren selbst (und damit auch der Algorithmus) muss unter höchsten Sicherheitsanforderungen betrieben werden. Auch nähere Angaben zur Wohnanschrift dürfen auf keinen Fall an die Auswertungsstelle weitergegeben werden, da damit der Zweck der Aufspaltung des Krebsregisters in Vertrauensstelle und Auswertungsstelle komplett unterlaufen würde. Bereits die Information über die Zugehörigkeit zu einem Ortsteil würde die Wiederherstellung des Personenbezugs in vielen Fällen wesentlich erleichtern. Bei seltenen Krebserkrankungen in einem zahlenmäßig beschränkten Kreis von Betroffenen und der

Kenntnis von Geschlecht und Geburtsjahr wären so zahlreiche Datensätze leicht reidentifizierbar. Erst recht darf keine Übermittlung von Gauß-Krüger-Koordinaten an die Auswertungsstelle erfolgen, denn dadurch ist die Wohnadresse der betroffenen Person eindeutig feststellbar. Die Folge wäre, dass direkt personenidentifizierende Daten, also Identitätsdaten, in der Auswertungsstelle vorhanden wären.

Wir setzten uns daneben für gesetzliche Klarstellungen entsprechend der Regelungen in Hamburg und dem Saarland dafür ein, welche Daten jeweils in der Vertrauensstelle und in der Auswertungsstelle des Bremer Krebsregisters gespeichert werden dürfen und welche der in der Auswertungsstelle gespeicherten Daten an Dritte übermittelt werden dürfen. Taggenaue Daten, wie zum Beispiel das Datum der ersten Tumordiagnose sollten nicht an die Auswertungsstelle übermittelt werden, um das Reidentifizierungsrisiko der Betroffenen zu minimieren. Für die Aufgaben der Auswertungsstelle reicht die Angabe von Monat und Jahr aus. Auch die Erforderlichkeit der Aufbewahrung der Identitätsdaten für einen Zeitraum von 30 Jahren nach dem Tod der Betroffenen ist aus unserer Sicht nicht gegeben.

Im Übrigen halten wir es für erforderlich, im Gesetz konkretisierende Regelungen zu den Modalitäten der Auswertungen sowie zu den jeweiligen Empfängern der Auswertungen zu treffen. Insbesondere scheint uns hier eine Beschränkung der Datenübermittlungsbefugnis an Forschungseinrichtungen allein zum Zweck der unabhängigen wissenschaftlichen Forschung notwendig. Die aktuelle Regelung eröffnet die Möglichkeit zur Übermittlung der Daten der Auswertungsstelle an Wirtschaftsunternehmen, die unter anderem auch – aber nicht notwendig im konkreten Fall – Vorhaben der unabhängigen wissenschaftlichen Forschung durchführen. Dafür soll ein berechtigtes Interesse der jeweiligen Einrichtung an den Daten ausreichen. Berechtigte Interessen können wirtschaftliche ebenso gut wie ideelle Interessen sein. Dies halten wir für hoch problematisch, da es sich bei den in der Auswertungsstelle gespeicherten Daten nicht um anonymisierte Daten handelt. Durch Hinzufügen des gegebenenfalls beim anfragenden Unternehmen aus anderen Zusammenhängen vorliegenden Zusatzwissens wird die Wiederherstellung des Personenbezugs in vielen Fällen leicht möglich sein.

Die im Gesetzentwurf enthaltene Regelung, wonach behandelnde Einrichtungen diagnostische Befundunterlagen ihrer Patientin bei Anzeichen für das Auftreten einer Krebserkrankung zwischen zwei Untersuchungen im Rahmen des Mammographie-Screenings auf Anforderung in pseudonymisierter Form an das Referenzzentrum Mammographie-Screening übermitteln müssen, halten wir für problematisch. Eine Übermittlung von Patientenunterlagen durch behandelnde Ärzte an die Einrichtungen des Mammographie-Screening-Programms ohne Einwilligung und ohne vorherige Information der betroffenen Patientinnen stellt einen erheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen dar, der im Hinblick auf den Zweck einer lückenlosen Qualitätssicherung des Programms unverhältnismäßig ist. Eine solche gesetzliche Verpflichtung anstelle einer Ermächtigung der behandelnden Ärztinnen und Ärzte hätte zur Folge, dass diese keine Möglichkeit hätten, im Einzelfall von einer Datenübermittlung abzusehen, selbst wenn ihnen bekannt wäre, dass ihre Patientin damit nicht einverstanden wäre. Dies würde auch zu einer unangemessenen Belastung des Arzt-Patienten-Verhältnisses führen. Wir halten es daher für dringend erforderlich, die Übermittlung von einer Einwilligung der Betroffenen abhängig zu machen. Für den Fall, dass diese Regelung gleichwohl vom Gesetzgeber gewollt sein sollte, schlugen wir vor, Maßnahmen zu treffen, um die Regelung im Hinblick auf die Eingriffsintensität etwas zu entschärfen. Zum einen sollte in diesem Fall unbedingt eine Verpflichtung zur vorherigen Information der Betroffenen durch die behandelnde Einrichtung in das Gesetz aufgenommen werden. Über eine entsprechende Datenübermittlung würde dann zumindest gegenüber der betroffenen Frau Transparenz geschaffen. Andererseits sollte aus der Übermittlungspflicht der behandelnden Einrichtung eine Übermittlungsbefugnis werden, um den jeweiligen behandelnden Ärztinnen und Ärzten im Einzelfall die Möglichkeit zu geben, von der Übermittlung absehen zu können.

6.2 Kinder- und jugendpsychiatrische Versorgungsdokumentationen

Im Berichtsjahr erfuhren wir, dass im Klinikum Bremen-Ost jährlich eine kinder- und jugendpsychiatrische Versorgungsdokumentation für das Land Bremen erstellt wird. Zu diesem Zweck wurden von den Ambulanzen und Stationen, die in diesem Bereich tätig sind, und dem Gesundheitsamt umfangreiche Dokumentationsbögen zu jedem Behandlungsfall ausgefüllt und an das Klinikum Bremen-Ost zum Zweck der Auswertung übermittelt. In diesen Bögen wurden von jeder Patientin und jedem Patienten Name, detaillierte Informationen über Diagnosen, Behandlungen, soziale Auffälligkeiten und das soziale und familiäre Umfeld gespeichert. Anschließend wurden die Bögen an eine Auswertungsstelle im Klinikum Bremen-Ost weitergegeben. Eine Einwilligung der Betroffenen wurde dafür nicht eingeholt. Die Veröffentlichung der Auswertungen erfolgte in aggregierter und anonymisierter Form.

Wir erörterten das Verfahren ausführlich mit Vertretern des Klinikums Bremen-Ost und der kinderpsychiatrischen Behandlungsstelle des Gesundheitsamtes Bremen. Unsere datenschutzrechtliche Bewertung ergab, dass das bislang praktizierte Verfahren Patientendaten und Klientendaten in unzulässiger Weise verarbeitet.

In Bezug auf die Datenverarbeitung durch das Gesundheitsamt bestehen bereits erhebliche Zweifel an der Erforderlichkeit der Erhebung eines derart detaillierten Datenkatalogs für die Aufgabenerfüllung. Nach dem Gesundheitsdienstgesetz (ÖGDG) bedarf die Verarbeitung personenbezogener Daten bei der freiwilligen Inanspruchnahme von Beratungsangeboten in jedem Fall der Einwilligung des Betroffenen. Zudem ist sicherzustellen, dass eine Beratung auch ohne Preisgabe personenbezogener Daten erfolgen kann. Es ist daher davon auszugehen, dass zumindest in der überwiegenden Zahl der Fälle bereits für die Datenerhebung, also das Ausfüllen der umfangreichen Dokumentationsbögen, eine Einwilligung der Betroffenen erforderlich ist. In jedem Fall unzulässig war die Weitergabe der Dokumentationsbögen an das Klinikum Bremen-Ost. Da eine Weitergabe der Identitätsdaten insoweit nicht erforderlich ist, forderten wir, das Verfahren derart umzustellen, dass die Daten nur bei Vorliegen einer Einwilligung und Schweigepflichtentbindung der Betroffenen in pseudonymisierter Form weitergegeben werden.

Die Erhebung des in den Dokumentationsbögen enthaltenen Datenkatalogs entspricht nach Auskunft des Klinikums Bremen-Ost dem fachlichen Standard in der medizinischen Behandlung. Eine Erhebung und Erfassung im Krankenhaus wäre demnach zum Zweck der Behandlung erforderlich und damit nach dem Krankenhausdatenschutzgesetz zulässig. Unzulässig war jedoch die Weitergabe der Dokumentationsbögen mitsamt den Identitätsdaten der Betroffenen an die Auswertungsstelle innerhalb des Klinikums Bremen-Ost. Eine solche Weitergabe innerhalb eines Krankenhauses ist nach dem Krankenhausdatenschutzgesetz nur in pseudonymisierter Form zulässig. Eine klinikübergreifende Weitergabe der Dokumentationsbögen ist nach dem Krankenhausdatenschutzgesetz ohne Einwilligung der Betroffenen, auch in pseudonymisierter Form, nicht zulässig. Dazu bedürfte es der Einwilligung und Schweigepflichtentbindung der Betroffenen.

Wir baten darum, den Dokumentationsbogen so zu verändern, dass die Wiederherstellung eines Personenbezugs allein anhand der medizinischen Daten so weit wie möglich erschwert wird. Deshalb sollte auf die Erhebung von taggenauen Daten zur Behandlung und auf die Erhebung des Geburtsdatums und der Nationalität verzichtet werden. Weiterhin muss auf die Erhebung von Daten, die für die Erstellung der Auswertungen nicht verwendet werden, verzichtet werden.

Wir forderten vom Gesundheitsamt und dem Klinikum Bremen-Ost die Umsetzung der von uns vorgeschlagenen Änderungen, die Erstellung einer Verfahrensbeschreibung nach dem Bremischen Datenschutzgesetz und die Erarbeitung der erforderlichen Einwilligungserklärungen und Schweigepflichtentbindungserklärungen. Die von uns geforderte Löschung der Identitätsdaten der Betroffenen in der Auswertungsstelle des Klinikums Bremen-Ost

wurde uns bereits bestätigt. Eine Umsetzung der übrigen Anforderungen war bis Redaktionsschluss noch nicht erfolgt.

6.3 Übersendung von Fotodokumentationen an eine Krankenkasse

Im Januar 2014 erhielten wir einen Hinweis, dass möglicherweise von der Allgemeinen Ortskrankenkasse (AOK) Bremen/Bremerhaven Fotodokumentationen erhoben würden, um bei der Prüfung von Kostenvoranschlägen für Hilfsmittel eine Begutachtung durch den Medizinischen Dienst der Krankenversicherung (MDK) nach Aktenlage zu ermöglichen. Auf unsere Nachfrage hin bestätigte die Krankenkasse diese Vorgehensweise für den Bereich Orthopädie-Technik und wies darauf hin, dass im Bereich Reha-Technik/Homecare zwar von ihr keine Fotodokumentationen bei den Leistungserbringern angefordert, diese aber zum Teil unaufgefordert von den Leistungserbringern übersandt würden. In diesen Fällen würden die Fotos nach der Prüfung durch den MDK an die jeweiligen Leistungserbringer wieder zurückgesandt.

Wir teilten der AOK Bremen/Bremerhaven mit, dass wir im Zusammenhang mit dieser Verfahrensweise datenschutzrechtlichen Änderungsbedarf sahen. Nach dem Sozialgesetzbuch V ist die Krankenkasse befugt, in geeigneten Fällen durch den MDK prüfen zu lassen, ob ein Hilfsmittel erforderlich ist. In diesen Fällen erhebt der MDK die für seine Prüfung beziehungsweise Begutachtung erforderlichen Daten direkt beim Leistungserbringer. Allerdings sind die Versicherten gegenüber dem Leistungserbringer gesetzlich nicht verpflichtet, an etwaigen Fotodokumentationen mitzuwirken. Daher forderten wir die AOK Bremen/Bremerhaven auf, sicherzustellen, dass die Sanitätshäuser die Betroffenen ausreichend darüber informieren, dass das Erstellen der Bilder freiwillig ist, welchem Zweck es dient und welche Vorteile es für die Versicherten mit sich bringt. Nur auf der Grundlage einer solchen informierten Einwilligung durch die Betroffenen dürfen Leistungserbringer solche Bilddaten erheben, speichern und zu gegebener Zeit verwenden. Zudem sollten Fotos, die nicht beziehungsweise nicht mehr benötigt werden, umgehend gelöscht beziehungsweise vernichtet werden. Wir wiesen darauf hin, dass im Fall eines Gutachtenauftrages an den MDK die Krankenkasse selbst unter keinen Umständen Kenntnis von der Fotodokumentation erhalten dürfe. Akzeptabel wäre in dieser Hinsicht lediglich, dass die Krankenkasse die Bilder in einem bereits vom Leistungserbringer verschlossenen gesonderten Umschlag, der eindeutig an den MDK adressiert ist, an den Gutachterdienst weiterleitet. Die AOK Bremen/Bremerhaven sagte uns die Umsetzung dieser Anforderungen zu.

6.4 Datenschutz in einer Apotheke

Eine Bürgerin meldete sich im Juli des Berichtsjahres bei uns und schilderte eine Situation in einer Apotheke, in der sie ihre Privatsphäre verletzt sah. Die Betroffene löste in der Apotheke ein Rezept für Psychopharmaka ein, die ihr aufgrund einer schweren chronischen Erkrankung verschrieben worden waren. Die Apotheke war zu diesem Zeitpunkt sehr voll, es bildeten sich Warteschlangen und auch am benachbarten Verkaufstresen wurden Kunden bedient. Die Apothekenmitarbeiterin holte die drei verschriebenen Medikamente aus dem Lager, legte sie dann gut sichtbar auf den Verkaufstresen und nannte auch für Dritte deutlich hörbar den Namen der Kundin und die Bezeichnungen aller drei Medikamente einschließlich der jeweiligen Dosis der Präparate.

Wir wiesen die Apotheke darauf hin, dass die dort verarbeiteten Gesundheitsdaten als besondere Arten personenbezogener Daten und der beruflichen Schweigepflicht unterliegende Daten gegen eine unberechtigte Kenntnisnahme durch Dritte besonders zu schützen sind. Die Erhebung, Verarbeitung und Nutzung dieser Daten – zu der auch eine Offenbarung gegenüber Dritten gehört – ist nur zulässig, soweit es gesetzlich erlaubt oder angeordnet ist oder die beziehungsweise der Betroffene eingewilligt hat. Zudem muss der Verkaufsraum einer Apotheke nach der Apothekenbetriebsordnung so eingerichtet sein, dass die Vertraulichkeit der Beratung, insbesondere an den Stellen, an denen Arzneimit-

tel an Kunden abgegeben werden, so gewahrt wird, dass das Mithören des Beratungsgesprächs durch andere Kunden weitestgehend verhindert wird. Wir forderten die Apotheke deshalb auf, technische und organisatorische Maßnahmen zu treffen, um eine unbefugte Kenntnisnahme der Gesundheitsdaten bei der Ausgabe von Medikamenten durch Dritte zu verhindern.

Die Inhaber der Apotheke zeigten sich sehr kooperativ und wiesen darauf hin, dass grundsätzlich die Patienten bei Erhalt des Rezeptes mit Namen angesprochen und die verordneten beziehungsweise gewünschten Medikamente mit ihrer Dosierung genannt würden, um der Beratungspflicht nach der Apothekenbetriebsordnung nachzukommen und eine Verwechslung auszuschließen. Dieses Verfahren wurde von uns als sachgerecht und angemessen bewertet, sofern zur Wahrung des Datenschutzes weitere Maßnahmen getroffen werden. Insbesondere ist sicherzustellen, dass wartende Kunden einen ausreichenden Abstand zum Verkaufstresen einhalten, um die dort geführten Beratungsgespräche nicht mit anhören zu können, beispielsweise durch eine Markierung am Fußboden und ein Schild mit dem Hinweis auf „Diskretion“ beziehungsweise „Abstand“. Zudem sind Maßnahmen zu treffen, die gewährleisten, dass die Beratungsgespräche am Verkaufstresen in gedämpfter Lautstärke geführt werden, um ein Mithören an der Kasse direkt nebenan zu verhindern.

Unsere Vorschläge wurden sofort aufgegriffen. Es wurde eine Datenschutzunterweisung für alle Mitarbeiterinnen und Mitarbeiter durchgeführt und an allen Kassen wurden mithilfe von Markierungen am Boden Diskretionszonen eingerichtet. Diese Maßnahmen sind nach unserer Bewertung ausreichend und angemessen.

6.5 Ordnungswidrigkeitsverfahren wegen der Lieferung von Rezeptdaten

Gegen ein großes Bremer Rechenzentrum betrieben wir ein Ordnungswidrigkeitsverfahren, das zur Verhängung eines Bußgeldes führte. Das Rechenzentrum hatte unbefugt und zumindest fahrlässig in hoher Anzahl in ärztlichen Verordnungen enthaltene Datensätze an ein Unternehmen übermittelt, das sich auf die Analyse großer Datensätze spezialisiert hat. Die Datensätze waren dem Rechenzentrum zu Abrechnungszwecken überlassen worden. Vor der Übermittlung hatte das Rechenzentrum die in der Verordnung enthaltenen Namen und Adressen zwar gelöscht. Die Ärztedaten, Apothekerdaten und Versichertendaten waren jedoch mithilfe eines Verschlüsselungsverfahrens lediglich pseudonymisiert worden.

Eine Pseudonymisierung personenbezogener Daten dient dem Zweck, die Bestimmung der betroffenen Person auszuschließen oder wesentlich zu erschweren, ein Rückbezug auf die jeweilige Person bleibt jedoch möglich. Als anonym sind Daten demgegenüber zu bezeichnen, wenn sich ein Rückbezug nicht oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft herstellen lässt.

Dem Unternehmen, dem die Daten übermittelt worden waren, war ein Rückbezug auf die betroffenen Ärztinnen und Ärzte, Apothekerinnen und Apotheker und Versicherten möglich, da es durch vorhergehende Übermittlungen über ein Zusatzwissen verfügte, das es ihm ermöglichte, die Daten zu entschlüsseln.

7. Soziales

7.1 Kindergarten Online [Ki ON]

Bereits im letzten Jahresbericht (vergleiche 36. Jahresbericht, Ziffer 7.6) berichteten wir über die datenschutzrechtlichen Probleme im Zusammenhang mit der Einführung des Fachverfahrens Kindergarten Online [Ki ON] in den Kindertagesstätten in Bremen. Leider konnten im Berichtsjahr 2014 im Hinblick auf die von uns benannten datenschutzrechtlichen Mängel keine wesentlichen Verbesserungen erreicht werden. Die senatorische Behörde

verkennt weiterhin die im Sozialgesetzbuch VIII festgelegte Garantenstellung der öffentlichen Vertragspartner zur Sicherstellung eines dem Sozialgesetzbuch entsprechenden Datenschutzniveaus bei der Inanspruchnahme freier Träger für den Betrieb von Kindertagesstätten. Auf Wunsch der senatorischen Behörde organisierten wir zu dieser Rechtsfrage einen Meinungsaustausch im Kreis der Datenschutzbeauftragten der Länder und des Bundes, in dem keines der sieben Länder, die sich am Meinungsaustausch beteiligten, die Auffassung der senatorischen Behörde teilte. Auch dies konnte die senatorische Behörde zu unserem großen Bedauern nicht zum Umdenken bewegen.

Für eine Auftragsdatenverarbeitung mit Sozialdaten bestehen nach dem Sozialgesetzbuch besondere Voraussetzungen, die von den in Anspruch genommenen Trägern erfüllt werden müssen (vergleiche dazu die Ausführungen unter Ziffer 7.6 im 36. Jahresbericht). Diese Voraussetzungen sind im vorliegenden Fall noch immer nicht erfüllt. Daher ist die Beauftragung einer privaten Firma mit dem Betrieb des Systems [Ki ON] im Wege der Auftragsdatendatenverarbeitung aus unserer Sicht weiterhin unzulässig.

Der Katalog der im [Ki ON] gespeicherten personenbezogenen Daten befindet sich noch in der Abstimmung zwischen der senatorischen Behörde und uns.

Die technischen Sicherheitsanforderungen, insbesondere die erforderliche starke Authentifizierung, sind bisher nicht erfüllt: Obwohl das Verfahren [Ki ON] zur Identifizierung und Authentifizierung von Nutzerinnen und Nutzern die Möglichkeit bietet, einen elektronischen Schlüssel (englisch: Token) zur Verhinderung einer unberechtigten Nutzung des Systems einzubinden, wird dieser bislang nicht genutzt. Außerdem müssen die Zugangsdaten sicher übertragen und eine den BSI-Normen (Normen des Bundesamtes für Sicherheit in der Informationstechnik) entsprechende Passwortkomplexität erzwungen werden.

Gegenwärtig haben alle bei dem Dienstleister in der Kundenbetreuung arbeitenden Mitarbeiterinnen und Mitarbeiter lesenden und schreibenden Zugriff auf das System. Demgegenüber ist erforderlich, hinsichtlich der Zugriffe eine differenzierte Berechtigungsvergabe vorzunehmen und bei Supportanfragen die Authentifizierung der Mitarbeiterinnen und Mitarbeiter über ein gesichertes Verfahren zu gewährleisten. Darüber hinaus muss eine individuelle Freischaltung durch die Mitarbeiterinnen und Mitarbeiter zur Ausübung von Supportfunktionen eingerichtet und Kriterien definiert werden, nach denen der Support jeweils auf die Server zugreift. Die Anwendungsadministration muss von der Supportfunktion getrennt werden. Im Rahmen möglicher Downloads muss die Zweckbindung sichergestellt werden. Schnittstellen und deren Absicherung für die Datenübermittlung an die senatorische Dienststelle sowie die technische Abschottung gegenüber Zugriffen der senatorischen Dienststelle müssen beschrieben und entsprechend abgesichert werden. Für den Rechenzentrumsbetrieb der privaten Firma muss zumindest der Nachweis über eine datenschutzkonforme Administration der Systemkomponenten und eine entsprechende Durchführung von Wartungsaufgaben geführt werden. Insbesondere müssen die wirksame Absicherung gegenüber Clouddiensten und ein effektives Revisionsverfahren garantiert sein. Um zu verhindern, dass mit nicht zugelassenen Geräten unzulässig auf die Daten zugegriffen werden kann, müssen diese standardmäßig über Maschinenzertifikate authentifiziert werden. Für alle Systemebenen müssen Administrationsfunktionen, mit denen unterhalb der vergebenen Berechtigungen für die Anwendungsbereiche des Systems auf das System zugegriffen werden kann, beschrieben und von Supportrollen und/oder Entwicklungsrollen abgegrenzt werden. Im Rahmen der Systementwicklung darf nicht auf Echtdaten zugegriffen werden. Ein Revisionsprozess muss implementiert werden. Die Auftraggeber müssen entsprechend der geltenden Rechtslage Auftragskontrollen durchführen und dies dokumentieren.

7.2 Datenfluss von privatem Träger an das Jobcenter

Es wandte sich ein Bürger an uns, der eine selbstständige Tätigkeit aufnehmen wollte und dafür einen Antrag auf Existenzförderung beim Jobcenter Bremen gestellt hatte. Im Rah-

men dieses Antrags hatte das Jobcenter für ihn einen Beratungstermin bei einem Verein vereinbart, der die Tragfähigkeit des Vorhabens für eine Selbstständigkeit prüfen sollte. Der Betroffene war von dem Verein aufgefordert worden, eine Einwilligung in die Datenverarbeitung abzugeben, was er unter ausdrücklichem Hinweis darauf ablehnte, dass er keinen Datenaustausch zwischen dem Verein und dem Jobcenter Bremen oder einem anderen Dritten wünschte. Der Verein wertete dies in einem dem Jobcenter übersandten Vermerk als Verweigerung der Zusammenarbeit. Zudem teilte der Verein dem Jobcenter mit, dass dort die persönliche Eignung des Betroffenen für fraglich gehalten werde. Der Antrag auf Existenzförderung wurde vom Jobcenter schließlich abgelehnt.

Der Betroffene bat darum, die in diesem Zusammenhang erfolgte Datenübermittlung durch den Verein an das Jobcenter Bremen datenschutzrechtlich zu überprüfen. Wir wandten uns an den Verein und baten um Mitteilung, zu welchem Zweck die Übermittlung der personenbezogenen Daten des Betroffenen an das Jobcenter erforderlich war und welche Rechtsgrundlage diese Datenübermittlung erlaube. Da die Datenübermittlung durch den Verein in unverschlüsselter Form per E-Mail erfolgt war, wiesen wir diesen zudem darauf hin, dass die Übermittlung von personenbezogenen Daten in unverschlüsselter Form per E-Mail nicht den Anforderungen an eine datenschutzgerechte Übermittlung nach dem Bundesdatenschutzgesetz entspricht, wonach, soweit personenbezogene Daten automatisiert verarbeitet oder genutzt werden, die innerbetriebliche Organisation so zu gestalten ist, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Diesbezüglich baten wir den Verein darum, die notwendigen technischen und organisatorischen Maßnahmen zu treffen um sicherzustellen, dass die oben genannten gesetzlichen Anforderungen zukünftig eingehalten werden. Zudem wiesen wir darauf hin, dass der in dem vom Verein bereitgestellten Formular vorhandene Passus „Einverständniserklärung“ nicht den gesetzlichen Wirksamkeitsvoraussetzungen an eine datenschutzrechtliche Einwilligung genügt. Das Gesetz fordert die Freiwilligkeit der Erklärung, eine umfassende Erläuterung des Zwecks der Erhebung, Verarbeitung und Nutzung sowie der Folgen der Verweigerung der Erklärung. Wir baten insoweit um Überarbeitung der Formulare.

Zur Datenübermittlung an das Jobcenter teilte der Verein lediglich mit, dass er eine Pflicht zur Mitteilung gegenüber dem Kooperationspartner habe, und dies nicht den Wünschen der Kundin oder des Kunden unterliege. Das Formular mit der Einwilligungserklärung wurde überarbeitet und uns in der geänderten Fassung zur Prüfung übersandt.

In Bezug auf die Datenübermittlung an das Jobcenter wiesen wir den Verein auf die Notwendigkeit einer Rechtsgrundlage für die Datenübermittlung hin, die im konkreten Fall nicht vorlag, da weder eine Rechtsvorschrift existiert, die die Datenübermittlung erlaubt noch eine Einwilligungserklärung des Betroffenen vorlag. Wir erläuterten, dass die Abgabe einer solchen Erklärung nicht zur Voraussetzung für eine Tragfähigkeitsbewertung durch den Verein gemacht werden kann, da dann keine Freiwilligkeit und infolgedessen keine rechtswirksame Einwilligung vorliegen würde. Folge der Verweigerung der Einwilligung in die Datenübermittlung kann deshalb lediglich sein, dass dem Betroffenen die Unterlagen selbst ausgehändigt werden. Er wäre dann selbst in der Lage zu entscheiden, ob er sie dem Jobcenter übergeben möchte oder nicht. An dem überarbeiteten Formular „Beratungsauftrag“ sahen wir noch Änderungsbedarf im Hinblick auf die Kennzeichnung von Telefonnummer und E-Mail-Adresse als freiwillige Angaben. An der Erforderlichkeit der Angaben Familienstand, Alter und Anzahl der Kinder äußerten wir Zweifel. Auch der Passus „Einwilligungserklärung“ genügte noch nicht den datenschutzrechtlichen Anforderungen. Es fehlte weiterhin an der Freiwilligkeit und an einer umfassenden Erläuterung des Zwecks

der Datenerhebung, Datenverarbeitung und Datennutzung. Wir baten darum zu bestätigen, dass von entsprechenden Datenübermittlungen ohne wirksame Einwilligung der beziehungsweise des Betroffenen zukünftig abgesehen wird. Zudem baten wir um Bestätigung, dass zukünftig von einer Übermittlung von personenbezogenen Daten in unverschlüsselter Form per E-Mail abgesehen wird und auch das Formular „Beratungsauftrag“ auf der Homepage zukünftig nur über eine sichere Website in verschlüsselter Form elektronisch versandt wird.

Nach einigem Hin und Her beauftragte der Verein eine Anwaltskanzlei, die für den Verein Folgendes mitteilte: Zukünftig würden Datenübermittlungen an das Jobcenter nur bei Vorliegen einer Einwilligung der Betroffenen erfolgen. E-Mails mit personenbezogenen Daten würden zukünftig nur noch in verschlüsselter Form übermittelt werden. Es werde auf der Homepage des Vereins eine verschlüsselte Verbindung für die elektronische Versendung der Formulare mit personenbezogenen Daten eingerichtet. Die Beantwortung der Fragen nach Familienstand, Anzahl und Alter der Kinder würde zukünftig freiwillig sein; diese Angaben würden verwendet, um den sozialen Druck und die finanziellen Belastungen der oder des Betroffenen einzuschätzen. Ebenso würden die E-Mail-Adresse und die Telefonnummer zukünftig auf freiwilliger Basis erhoben. Die Einverständniserklärung würde unseren Anforderungen entsprechend angepasst.

7.3 Das neue BAföG-System

Bereits im August 2012 formulierten wir unsere Anforderungen für die Einführung eines neuen Systems zur BAföG-Berechnung. Insbesondere unsere Anforderungen zur Ermittlung und Umsetzung der technisch erforderlichen Maßnahmen waren nicht oder nur zum Teil in dem Fachdatenschutzkonzept zur „Einführung der Software Dialog 21“ vom Mai 2013 enthalten. Im Februar des Berichtsjahres erhielten wir vom Studentenwerk eine Neufassung des Datenschutzkonzeptes. Darin fanden sich erneut unsere damals genannten Anforderungen nicht oder nur zum Teil wieder. Wir übergaben deshalb dem Studentenwerk noch einmal eine Bewertung des aktuellen Konzepts mit folgenden Inhalten:

In dem Konzept muss unter Beachtung der Voraussetzungen des Sozialgesetzbuch X dokumentiert werden, welche Datenverarbeitungsvorgänge im Wege der Auftragsdatenverarbeitung an welche Stellen vergeben werden. Es müssen konkrete Sperrfristen und Löschfristen festgelegt werden. Es muss eine Schutzbedarfsanalyse für die zu verarbeitenden Daten durchgeführt werden. Dabei müssen etwaige bereits durchgeführte Schutzbedarfsfeststellungen anderer verantwortlicher Stellen, die dieses Verfahren einsetzen, und daraus resultierende Maßnahmen eigenverantwortlich geprüft werden. Gegebenenfalls müssen eigene Festlegungen explizit definiert werden. Ebenso muss das Ergebnis der Risikoanalyse anderer Stellen daraufhin geprüft werden, ob die Gefährdungen vollständig ermittelt wurden und das Niveau der resultierenden Maßnahmen (Prüfung auf Vollständigkeit, Mechanismenstärke und Zuverlässigkeit) ausreicht. Die Analyse muss sich konkret auf die entsprechenden Komponenten des bremischen Studentenwerks beziehen.

Weitere Anforderungen formulierten wir zu den Themen Dokumentation, Netzkonzept, Zutritts-, Zugangs- und Zugriffs-, Weitergabe-, Eingabe- und Verfügbarkeitskontrolle.

Wir erwarten, dass das Studentenwerk, von dem wir im Berichtsjahr keine weitere Rückmeldung zu diesem Thema erhalten haben, seine datenschutzrechtliche Verantwortung wahrnehmen und unsere Anforderungen zeitnah umsetzen wird.

8. Bildung, Wissenschaft und Kultur

8.1 Übermittlung von Schülerdaten an Verlagsportal

Die Senatorin für Bildung und Wissenschaft hat für alle Grundschulen für ein Leseportal eine Landeslizenz erworben. In diesem Zusammenhang erhielten wir Kenntnis davon, dass

ein Lehrer einer Grundschule die vollständigen Namen der Schülerinnen und Schüler seiner Klasse ohne Einwilligung der Eltern an www.antolin.de angemeldet hatte. In dem Datenschutzhinweis des Verlags wird ausdrücklich auf die Einwilligung der Eltern und die Nutzung von Pseudonymen verwiesen. Wir haben erhebliche Zweifel daran, dass Einwilligungen von Eltern auf ihrer freien Entscheidung beruhen, da sie nach unseren Erfahrungen häufig bei einer Verweigerung oder einem späteren Widerruf der Einwilligung Nachteile für ihre Kinder befürchten. Daher sollten auf jeden Fall keine Klarnamen der Schülerinnen und Schüler verwendet werden.

Wir wiesen die Bildungsbehörde darauf hin und baten, mit dem Verlag einen Vertrag zur Auftragsdatenverarbeitung abzuschließen, der sicherstellt, dass sich Datenschutzverletzungen wie die beschriebene nicht wiederholen und keine Klarnamen bei der Nutzung des Leseportals mehr verwendet werden. Die Senatorin für Bildung und Wissenschaft kündigte daraufhin an, sie werde einen Vertrag mit dem Verlag abschließen, der unsere Anforderungen erfüllt. Außerdem erließ sie eine Verfügung zur datenschutzgerechten Nutzung von Internetlernportalen, die ebenfalls unseren Anforderungen gerecht wird.

8.2 Facebook-Präsenz auf der Homepage einer Schule

Aufgrund einer Eingabe erlangten wir Kenntnis darüber, dass eine Oberschule über eine Facebook-„Fanseite“ verfügte, auf die sie auf ihrer Homepage hinwies. Auf der Homepage forderte sie alle Eltern auf, Bilder und Videos an die Schule zu senden, damit diese auf die Facebook-„Fanseite“ der Schule gestellt werden könnten. In diesem Zusammenhang wiesen wir die Schule auf eine Verfügung der Senatorin für Bildung und Wissenschaft hin, in der diese alle Schulen angewiesen hatte, insbesondere Social Plugins (soziale Erweiterungsmodule) von Facebook von den schuleigenen Homepages zu entfernen. Dazu gehört auch, auf Verlinkungen zu verzichten.

Auf Nachfrage der Schulleitung erklärten wir, dass die Einrichtung einer Facebook-„Fanseite“ gegen das Bremische Schuldatenschutzgesetz verstößt. Es ist nicht erforderlich, über diesen Weg über schulinterne Angelegenheiten zu informieren, weil es ausreicht, darüber per Aushang, E-Mail oder auf der schuleigenen Internetseite zu informieren. Zudem werden alle Daten, die auf facebook-„Fanseiten“ zur Verfügung gestellt werden, bei Facebook als derjenigen Stelle verarbeitet, die diese Plattform betreibt. Die Schule als verantwortliche Betreiberin der „Fanseite“ müsste die technischen und organisatorischen Maßnahmen treffen, die den besonderen gesetzlichen Anforderungen gerecht werden. Insbesondere wäre zu gewährleisten, dass Unbefugte keine Kenntnis darüber erhalten, welche Personen welche Seiten der „Fanseite“ aufrufen. Diese Anforderungen könnte die Schule nicht erfüllen, weil Facebook den Betreibern der „Fanseiten“ dies technisch nicht ermöglicht. Sobald nämlich Erziehungsberechtigte oder Schülerinnen und Schüler solche Facebook-„Fanseiten“ aufrufen, werden ihre IP-Adressen bei Facebook gespeichert und mit anderen Facebook zur Verfügung stehenden Daten verknüpft. Dadurch ist für Facebook ein Bezug zu Personen herstellbar, die eine Profilseite bei Facebook betreiben. Darüber hinaus können auch Nichtmitgliedern des sozialen Netzwerks für Facebook erkennbar sein, da Facebook auf allen Seiten, die den Facebook-Button enthalten, einen Cookie mit zweijähriger Gültigkeit setzt. Dadurch kann Facebook auch bei diesen Personen das gesamte Internetverhalten speichern und Profile erstellen, die diese Personen für Facebook individualisierbar machen.

Die Schule räumte ein, dass die Aufforderung an die Eltern, Bilder und Videos für die Facebook-„Fanseite“ zur Verfügung zu stellen, nicht richtig war. Bisher seien keine Dokumente eingereicht worden. Außerdem habe sie die Facebook-Präsenz beendet, indem sie die Facebook-„Fanseite“ gelöscht habe.

8.3 Zusammenarbeit zwischen Schule, Jugendhilfe, Gesundheitsamt und ReBUZ

Das von der städtischen Deputation für Bildung beschlossene Konzept zur Beschulung von Schülerinnen und Schülern mit sonderpädagogischem Förderbedarf zur sozialen und

emotionalen Entwicklung soll die Grundsätze der Inklusion in den Schulen weiterentwickeln. Hierzu fordert das Bremische Schulgesetz auf, speziell mit regionalen Instituten zu kooperieren. Diese Aufgabe nehmen die Regionalen Beratungs- und Unterstützungszentren (ReBUZ) wahr. Ebenso verpflichten das Kinder- und Jugendhilfegesetz und das Sozialgesetzbuch VIII ausdrücklich zur Zusammenarbeit mit anderen Stellen und öffentlichen Einrichtungen sowie mit Stellen der Schulverwaltung, die alle mit einem unterschiedlichen Auftrag und Selbstverständnis auf Kinder und Jugendliche einwirken. Die Kooperationspartner tragen neben den Erziehungsberechtigten die gemeinsame Verantwortung für die Bildung und Erziehung junger Menschen. Hierbei gibt es vielfältige Überschneidungen in der Aufgabenwahrnehmung der jeweiligen Stellen. Da zur Zusammenarbeit dieser Stellen eine Vielzahl teils sensibler personenbezogener Schülerdaten und Sozialdaten ausgetauscht werden sollen, bat uns die Senatorin für Bildung und Wissenschaft um Stellungnahme zu dem Konzept.

Die vorliegende Vereinbarung stellt klar, dass ein Austausch zwischen den beteiligten Stellen zum Zweck einer gemeinsamen individuellen Förderplanung und Hilfeplanung für die betroffenen Schülerinnen und Schüler erfolgen soll. Als Rechtsgrundlage für den dafür erforderlichen Austausch personenbezogener Schülerdaten, Sozialdaten und Gesundheitsdaten soll eine Einwilligung der Betroffenen beziehungsweise deren Erziehungsberechtigten eingeholt werden. Dabei wird auf die Beachtung der jeweils einschlägigen datenschutzrechtlichen Vorschriften in den Sozialgesetzbüchern VIII und X sowie im Bremischen Schuldatenschutzgesetz hingewiesen. Für die Datenverarbeitung in den einzelnen vorgenannten Stellen soll durch die drei beteiligten senatorischen Dienststellen (Bildung, Gesundheit und Soziales) eine Verfahrensbeschreibung erstellt und den jeweiligen behördlichen Datenschutzbeauftragten zugeleitet werden.

Gegen die Festlegungen in der vorliegenden Vereinbarung zur Zusammenarbeit bestehen aus unserer Sicht keine Bedenken. Das Muster zur Erklärung zur Entbindung von der Schweigepflicht im vorgenannten Rahmen informiert über den Zweck der Datenverarbeitung und entbindet ausdrücklich die Mitarbeiterinnen und Mitarbeiter der jeweils zu nennenden Einrichtung von der Schweigepflicht. Dies sieht insbesondere vor, dass lediglich die erforderlichen Auskünfte eingeholt und Unterlagen zur Einsichtnahme herangezogen werden, um die Betroffene oder den Betroffenen umfassend beraten zu können und beschreibt die zweckgebundene Verwertung der Daten. Ergänzend dazu informiert eine weitere Erklärung zur Entbindung von der Schweigepflicht innerhalb des zuständigen Regionalen Beratungs- und Unterstützungszentrum (ReBUZ) darüber, dass dieses die einzelnen Fälle jeweils intern arbeitsteilig bearbeitet, und durch die Erklärung innerhalb des ReBUZ personenbezogene Daten unter den Mitarbeiterinnen und Mitarbeitern weitergegeben und ausgetauscht werden können. Auch dieses Formular nennt die entsprechenden Datenschutzvorschriften und die explizite Zweckbindung der Datenverarbeitung.

8.4 „Unkonventionelle“ Zahlungserinnerung durch einen Kulturverein

Mit der Zahlungsmoral einzelner Mitglieder eines Kulturvereins stand es nicht zum Besten. Der Vorstand des Vereins hatte daher eine Tabelle erstellt, in der die jeweils unbezahlten Mitgliedsjahresbeiträge jedes einzelnen seiner namentlich aufgeführten Vereinsmitglieder aufgelistet waren. Die Tabelle enthielt zudem eine eigene Spalte, in der jedem Beitragsschuldner eine Schuldnerrangplatzierung zuerkannt war. Zwecks Erinnerung an die Zahlung versandte der Vereinsvorstand diese Tabellenübersicht kurzerhand als Anhang einer E-Mail an alle Vereinsmitglieder. Damit erhielt nun jedes einzelne Mitglied nicht nur eine Übersicht über seine etwaigen eigenen Beitragsschulden gegenüber dem Verein, sondern zugleich auch Kenntnis über die etwaigen Beitragsschulden sämtlicher anderer Mitglieder. Darüber hinaus wurde die E-Mail nicht nur an private E-Mail-Empfängeradressen sondern zum Teil auch an sogenannte Funktionsadressen, also betriebliche oder dienstliche E-Mail-Postfächer einzelner Vereinsmitglieder, gesendet. Prompt meldete sich eine Mitarbeiterin eines Unternehmens und teilte dem Verein mit, dass das angeschriebene Ver-

einsmitglied nicht mehr im Unternehmen arbeite und aufgrund der eingerichteten automatischen E-Mail-Weiterleitung sie nun an dessen Stelle die Schuldnerliste erhalten habe.

Die Weitergabe personenbezogener Informationen zu Zahlungsrückständen einzelner Vereinsmitglieder an sämtliche andere Vereinsmitglieder und – im Falle der Weiterleitung aus Funktionspostfächern – an vereinsexterne Personen war selbstverständlich datenschutzrechtlich unzulässig. Denn weder lag eine Einwilligung eines jeden einzelnen Vereinsmitglieds in die Übermittlung der Information zum eigenen Beitragsrückstand an sämtliche andere Vereinsmitglieder vor, geschweige denn an weitere vereinsexterne Dritte, noch gab es eine gesetzliche Erlaubnisnorm für diese Informationsverteilung. Die einschlägige gesetzliche Befugnisnorm lässt zwar eine Übermittlung personenbezogener Daten unter anderem dann zu, wenn dies zur Durchführung eines Schuldverhältnisses erforderlich ist. Der Umstand, ob und gegebenenfalls in welchem Umfang ein Vereinsmitglied seinem Verein Beiträge schuldig ist, betrifft allerdings ausschließlich die Durchführung des Rechtsverhältnisses zwischen diesem Mitglied und dem eingetragenen Verein als eigenständiger juristischer Persönlichkeit, geht also andere nichts an. Nicht erforderlich und daher unzulässig war auch die Führung und Mitteilung von Schuldnerrangplätzen.

Nachdem wir dieses Vorgehen des Vereins unter näherer Erläuterung der datenschutzrechtlichen Rechtslage beanstandet hatten, zeigte sich der Vereinsvorstand einsichtig, entschuldigte sich für diese Panne und forderte alle Mitglieder zur Löschung der übermittelten Tabelle auf. Wir nahmen diesen Vorfall noch zum Anlass darauf hinzuweisen, dass nach Möglichkeit sensiblere personenbezogene Informationen nicht via unverschlüsselter E-Mail versendet werden sollten, da unverschlüsselte E-Mails auf ihrem Weg durchs Internet weder gegen eine Kenntnisnahme durch unbefugte Dritte noch gegen inhaltliche Veränderungen geschützt sind.

8.5 E-Mail-Nutzung bei der Senatorin für Bildung und Wissenschaft

Bereits im 34. Jahresbericht (siehe Ziffer 8.4) stellten wir die Problematik der Weiterleitung sensibler Daten von Schülerinnen und Schülern in Bezug auf die Verfahrensweise einer Privatschule dar. Wir nahmen dies zum Anlass, die senatorische Behörde um Auskunft über die entsprechende Verfahrensweise an öffentlichen Schulen zu bitten.

Die senatorische Behörde erklärte hierzu, dass eine Verschlüsselung und digitale Signatur von E-Mails über digitale Zertifikate und die Ausstattung aller Lehrkräfte mit dienstlichen E-Mail-Adressen bis Ende 2012 geplant sei (vergleiche 35. Jahresbericht, Ziffer 8.4). Da wir keine Umsetzungsbestätigung erhalten hatten, legten wir der senatorischen Behörde im Mai des Berichtsjahres einen umfangreichen Fragenkatalog vor. Dieser enthielt beispielsweise Fragestellungen zur Einführung persönlicher Nutzerzertifikate, zu möglicherweise verwendeten Zertifikatsfunktionen und zur Infrastruktur, bei der insbesondere die sichere Anbindung von häuslichen und/oder mobilen Arbeitsplätzen zu betrachten ist. Darüber hinaus enthielt der Katalog Fragen zur Verhinderung der Übertragung von E-Mails in andere lokale E-Mail-Systeme, zur Möglichkeit der lokalen Speicherung sensibler Daten von Schülerinnen und Schülern und der dafür gegebenenfalls erforderlichen Sicherheitskonfiguration. Darüber hinaus wurden Fragen zur Sicherstellung der ausschließlichen Nutzung dienstlicher E-Mail-Konten und zur Gewährleistung der Vertraulichkeit durch Verschlüsselungsverfahren sowie nach der Protokollierung administrativer Zugriffe gestellt. Dazu hat die senatorische Behörde Stellung genommen. Eine Prüfung der Stellungnahme konnte bis Redaktionsschluss noch nicht erfolgen.

8.6 Kündigung eines Abonnements mit unvorhergesehenen Schwierigkeiten

Eine Kulturinteressierte hatte ein Zeitabonnement für Veranstaltungen einer Kultureinrichtung. Aufgrund eingetretener gesundheitlicher Probleme konnte sie Veranstaltungen im Abonnementzeitraum nicht mehr besuchen. Das laufende Abonnement sollte daher gekündigt werden. Eine Angehörige der Abonnentin legte daher bei der Kultureinrichtung

ein ärztliches Attest vor und gab die Einrittskarten für die restlichen Abonnementveranstaltungen zurück. Gleichwohl kam es in der Folge zu einer weiteren Abbuchung der Abonnementgebühr vom Konto der Betroffenen. Ihr und ihren Angehörigen wurde seitens einer Mitarbeiterin der Kultureinrichtung mitgeteilt, dass aus dem ärztlichen Attest die Krankheitsdiagnose nicht zu ersehen sei. Man benötige die genaue ärztliche Diagnose, um prüfen zu können, ob man die Kündigung überhaupt akzeptiere. Nachdem sich die Kultureinrichtung auch bei nochmaliger Vorsprache einer Angehörigen geweigert hatte, den eingezogenen Betrag rückzuerstatten und auf ihrer Forderung der Vorlage einer ärztlichen Diagnose bestanden hatte, sah sich die Angehörige gezwungen, die Diagnose mitzuteilen, um den abgebuchten Betrag rückerstattet zu bekommen.

Auf welcher rechtlichen Grundlage die Kultureinrichtung meinte, ärztliche Diagnosedaten erheben zu dürfen, ist uns völlig unklar. Bei ärztlichen Diagnosedaten handelt es sich offensichtlich um persönlichste Gesundheitsinformationen, also besonders sensible Angaben. Sie genießen daher besonderen datenschutzrechtlichen, daneben auch berufsstandesrechtlichen (ärztliche Schweigepflicht) und schließlich sogar strafrechtlichen (§ 203 Strafgesetzbuch) Schutz. Sieht man von diesem Rechtsaspekt ab, so stellt sich tatsächlich auch die Frage, wie die ärztliche Diagnose seitens der medizinisch aller Voraussicht nicht fachkundigen Kundenverwaltung der Kultureinrichtung überprüft werden und schließlich die weitere Besuchsfähigkeit der Abonnentin eigenständig beurteilt werden soll. Wir haben die Kultureinrichtung daher angeschrieben und um Stellungnahme zu diesem Vorgehen gebeten.

9. Bau und Umwelt

9.1 Umgang mit Bauvorlagen beim Senator für Umwelt, Bau und Verkehr

Ein Petent beschwerte sich bei uns darüber, dass seine Nachbarn beim Senator für Umwelt, Bau und Verkehr Einsicht in seine Bauakte genommen hätten und dabei auch Kopien angefertigt worden seien. Der Bausenator stützte sein Vorgehen auf § 70 der Bremischen Landesbauordnung, wonach eine Beteiligung der Nachbarn vorgesehen ist, soweit deren Belange berührt sein können. Wir forderten den Bausenator auf, dem Petenten mitzuteilen, welche konkreten Kopien an wen herausgegeben worden sind. Zudem baten wir zwecks datenschutzrechtlicher Prüfung um Stellungnahme, inwieweit das Bauvorhaben des Petenten nachbarliche Belange berührt und ob die Nachbarn Einwendungen erhoben haben, denen nicht entsprochen worden ist. Die daraufhin erfolgte Antwort des Bausenators beantwortet unsere Fragen nicht abschließend. Eine vollständige Antwort steht noch aus.

9.2 Müllcontainer mit digitalem Zugang

Ein Petent teilte uns mit, dass sein Vermieter Müllcontainer mit digitalem Zugang einführen wolle. Er befürchtete dadurch eine Beeinträchtigung seines Rechts auf informationelle Selbstbestimmung, wenn erfasst werde, wer wie viel Müll an welchen Tagen, zu welchen Uhrzeiten und wie häufig entsorge. Auf Nachfrage teilte uns der Vermieter dazu mit, dass jeder Mietpartei ein individueller Transponderclip für die Abfallschleuse ausgehändigt werde, um die Zahl der Einwürfe zu erfassen und zu verhindern, dass unberechtigte Personen ihren Abfall in die Gefäße einwerfen. Auf dem Clip werde jeweils der Name der betroffenen Person, die dazugehörige Wohnung sowie die Häufigkeit der Einwürfe gespeichert. Die Elektronik in der Abfallschleuse erfasse jeden Zugriff auf die Schleuse und ordne sie über die Clipnummer der Mietpartei zu. Mit der Abrechnung werde die Anzahl der Zugriffe, bezogen auf den Gesamtfall, in die zu zahlende Gebühr umgerechnet. Wir forderten den Vermieter auf, uns für das Verfahren das zugehörige Datenschutzkonzept zu übersenden, um eine datenschutzrechtliche Prüfung vornehmen zu können. Eine Antwort vonseiten des Vermieters steht noch aus.

10. Finanzen

10.1 Umstellung von bargeldlosen Zahlungen auf SEPA

Bereits in den beiden vorangegangenen Berichtsjahren (vergleiche 35. Jahresbericht, Ziffer 10.2 und 36. Jahresbericht, Ziffer 11.1) begleiteten wir das bei der Senatorin für Finanzen angesiedelte Projekt SEPA (Single Euro Payments Area), dessen Ziel die Vereinheitlichung von bargeldlosen Zahlungen ist, sodass für Bankkundinnen und Bankkunden keine Unterschiede mehr zwischen nationalen und grenzüberschreitenden Zahlungen bestehen.

Zur Datenschutzdokumentation für das dort verwendete Verfahren TransX nahmen wir in diesem Berichtsjahr erneut Stellung und übermittelten unsere Anforderungen zur Gewährleistung des Datenschutzes. Leider erhielten wir bisher keine Rückmeldung dazu, ob unsere Anforderungen umgesetzt worden sind. Die Datenschutzdokumentationen für die Verfahren SEPA, Giro und FIKuS sowie für die Mandatsverwaltung sind nicht bei uns eingegangen. Weiterhin liegt zu Redaktionsschluss keine Information vor, ob die angekündigte Umsetzung der Berechtigungen für den Zahlungsverkehr im Rahmen des Projektes ReBe (Reorganisation Berechtigungen, vergleiche 36. Jahresbericht, Ziffer 4.2) erfolgt ist.

10.2 Zentrale Zuwendungsdatenbank

Über das Projekt zur Einführung einer zentralen Zuwendungsdatenbank (ZEBRA) berichteten wir bereits in der Vergangenheit (vergleiche 33. Jahresbericht, Ziffer 10.2, 34. Jahresbericht, Ziffer 11.2 und 36. Jahresbericht, Ziffer 11.2). In diesem Berichtsjahr erhielten wir erneut Unterlagen zur Datenschutzdokumentation, die mittlerweile sehr weit fortgeschritten ist. Einzelne Punkte zu den technischen und organisatorischen Maßnahmen sind noch zu klären. Wir gehen davon aus, dass dies zeitnah möglich sein wird.

Unsere Hinweise zum Rechtekonzept und Rollenkonzept werden derzeit zwischen dem behördlichen Datenschutzbeauftragten der Senatorin für Finanzen und der Projektleitung beraten. Wir gehen davon aus, dass unsere Anmerkungen zum Rechtekonzept und Rollenkonzept geklärt werden können, unsere Anmerkungen zum Datenschutz Eingang in die Verfahrensgestaltung finden und dass wir bei Zweifelsfragen wieder beteiligt werden. Weiterhin legten wir unsere Anforderungen an die Realisierung der Schnittstelle zum Fachverfahren SAP dar. Diese Schnittstelle soll im ersten Quartal 2015 aktiv werden. Wir nehmen an, dass unsere Hinweise berücksichtigt und durch geeignete Maßnahmen unter Mitwirkung des behördlichen Datenschutzbeauftragten umgesetzt werden.

11. Medien/Telemedien

11.1 „Google-Urteil“ des Europäischen Gerichtshofs

Der Europäische Gerichtshof (EuGH) entschied in seinem Urteil vom 13. Mai 2014, dass und unter welchen Voraussetzungen Suchmaschinenbetreiber auf ihren Ergebnislisten Links zu Internetseiten löschen müssen, auf denen personenbezogene Daten gespeichert werden oder wurden. Die Datenschutzbeauftragten des Bundes und der Länder verwiesen in ihrer Entschließung „Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen“ darauf, dass dieses für den Grundrechtsschutz maßgebliche Urteil nunmehr von den Suchmaschinenbetreibern umfassend umgesetzt werden müsse. Zu Recht werde in der Debatte auf die erhebliche Macht der Anbieter von Suchmaschinen hingewiesen, über die Veröffentlichung von Suchergebnissen zu entscheiden. Diese Macht bestehe jedoch nicht erst seit der Entscheidung des EuGH. Anbieter von Suchmaschinen seien keine neutralen Sachwalter der Informationsgesellschaft, sondern kommerziell handelnde Wirtschaftsunternehmen. Welche Suchergebnisse den Nutzern angezeigt würden, bestimme sich damit jedenfalls auch nach den kommerziellen Interessen von Suchmaschinen und ihren Vertragspartnern. Darüber hinaus unterlägen Suchmaschinen auch bereits

vor der Entscheidung des EuGH bei der Gestaltung der Suchergebnisse äußeren Beschränkungen (zum Beispiel durch das Urheberrecht). Mit dem Urteil werde klargestellt, dass Suchmaschinen neben diesen Erwägungen jetzt auch die Grundrechte der Betroffenen zu berücksichtigen hätten (vergleiche die Entschließung unter Ziffer 19.10 dieses Berichts).

Im Einzelnen enthält die Entscheidung des EuGH die im Folgenden dargestellten Festlegungen: Der Betreiber einer Internetsuchmaschine sei verantwortlich für die von ihm vorgenommene Verarbeitung personenbezogener Daten, die auf von Dritten veröffentlichten Internetseiten erschienen. Das automatische, kontinuierliche und systematische Aufspüren von Daten durch den Betreiber einer Suchmaschine (beispielsweise Google), die dieser dann mit seinem Indexprogramm auslese, speichere und organisiere, auf seinen Servern aufbewahre und in Form von Ergebnislisten an seine Nutzerinnen und Nutzer weitergebe und diesen bereitstelle, sei eine Erhebung und damit eine Verarbeitung von personenbezogenen Daten im Sinne der Europäischen Datenschutzrichtlinie. Weil der Suchmaschinenbetreiber über die Zwecke und Mittel einer solchen Verarbeitung entscheide, sei er Verantwortlicher im Sinne der Richtlinie.

Die Tätigkeit einer Suchmaschine erfolgt nach Auffassung des Europäischen Gerichtshofes zusätzlich zu der der Herausgeber von Websites. Durch sie könnten die Grundrechte auf Achtung des Privatlebens und Schutz personenbezogener Daten erheblich beeinträchtigt werden. Aus diesem Grund habe der Suchmaschinenbetreiber in seinem Verantwortungsbereich im Rahmen seiner Befugnisse und Möglichkeiten dafür zu sorgen, dass seine Tätigkeit den Anforderungen der Richtlinie entspreche. Nur so könnten die in der Richtlinie vorgesehenen Garantien ihre volle Wirksamkeit entfalten und ein wirksamer und umfassender Schutz der betroffenen Personen, insbesondere des Privatlebens, tatsächlich verwirklicht werden.

Der Suchmaschinenbetreiber sei unter bestimmten Voraussetzungen verpflichtet, von der Ergebnisliste, die im Anschluss an eine anhand des Namens einer Person durchgeführte Suche angezeigt werde, Links zu von Dritten veröffentlichten Internetseiten mit Informationen über diese Person zu entfernen. Eine solche Verpflichtung könne auch bestehen, wenn der betreffende Name oder die betreffenden Informationen auf diesen Internetseiten nicht vorher oder gleichzeitig gelöscht würden, gegebenenfalls auch dann, wenn ihre Veröffentlichung dort als solche rechtmäßig gewesen sei.

Der Gerichtshof weist darauf hin, dass eine Verarbeitung personenbezogener Daten, die von einem Suchmaschinenbetreiber vorgenommen wird, es jeder Nutzerin oder jedem Nutzer ermöglicht, bei Durchführung einer Suche anhand des Namens einer natürlichen Person mit der Ergebnisliste einen strukturierten Überblick über die zu ihr im Internet verfügbaren Informationen zu erhalten. Diese beträfen zahlreiche Aspekte des Privatlebens und hätten ohne die Suchmaschine nicht oder nur sehr schwer miteinander verknüpft werden können. Somit könnten die Nutzerinnen und Nutzer des Internets ein mehr oder weniger detailliertes Profil der gesuchten Person erstellen. Die Wirkung des Eingriffs in die Rechte der betroffenen Person werde noch durch die bedeutende Rolle des Internets und der Suchmaschinen in der modernen Gesellschaft gesteigert, die den in den Ergebnislisten enthaltenen Informationen Allgegenwärtigkeit verliehen. Wegen seines potenziellen Gewichts kann ein solcher Eingriff nach Ansicht des Gerichtshofs nicht allein mit dem wirtschaftlichen Interesse des Suchmaschinenbetreibers an der Verarbeitung der Daten gerechtfertigt werden.

Gleichwohl könne sich die Entfernung von Links aus der Ergebnisliste aber je nach Information, um die es sich handele, auf das berechtigte Interesse von potenziell am Zugang zu der Information interessierten Nutzerinnen und Nutzern des Internets auswirken. Nach Ansicht des Gerichtshofs ist daher ein angemessener Ausgleich zwischen diesem Interesse und den Grundrechten der betroffenen Person, insbesondere des Rechts auf Ach-

tung des Privatlebens und des Rechts auf Schutz personenbezogener Daten, zu finden. Zwar überwiegen nach Auffassung des Europäischen Gerichtshofs die Rechte der betroffenen Person im Allgemeinen auch gegenüber dem Interesse der Internetnutzerinnen und Internetnutzer. Der Ausgleich könne in besonders gelagerten Fällen aber von der Art der betreffenden Information, von deren Sensibilität für das Privatleben der betreffenden Person und vom Interesse der Öffentlichkeit am Zugang zu der Information abhängen, das unter anderem je nach der Rolle, die die Person im öffentlichen Leben spiele, variieren könne.

Die betroffene Person könne verlangen, dass Links zu Internetseiten aus einer solchen Ergebnisliste gelöscht würden, weil die darin über sie enthaltenen Informationen nach einer gewissen Zeit „vergessen" würden. Auch könne es sein, dass die ursprünglich rechtmäßige Verarbeitung sachlich richtiger Daten im Laufe der Zeit nicht mehr den Bestimmungen der Richtlinie entspreche, etwa wenn die Daten in Anbetracht aller Umstände des Einzelfalls, insbesondere der verstrichenen Zeit, den Zwecken, für die sie verarbeitet worden seien, nicht entsprächen, dafür nicht mehr erheblich seien oder darüber hinausgingen. Eine betroffene Person könne verlangen, dass der Suchmaschinenbetreiber prüfe, ob sie ein Recht darauf habe, dass die betreffende Informationen über sie zum gegenwärtigen Zeitpunkt nicht mehr durch eine Ergebnisliste, die im Anschluss an eine anhand ihres Namens durchgeführte Suche angezeigt werde, mit ihrem Namen in Verbindung gebracht werde. In diesem Fall seien die Links der Internetseiten, die diese Informationen enthielten, aus der Ergebnisliste zu löschen, es sei denn, es lägen besondere Gründe vor, beispielsweise die Rolle der betreffenden Person im öffentlichen Leben, die ein überwiegendes Interesse der breiten Öffentlichkeit am Zugang zu diesen Informationen über eine solche Suche rechtfertigten.

Der Gerichtshof stellt klar, dass solche Anträge von der betreffenden Person unmittelbar an den Suchmaschinenbetreiber gerichtet werden könnten. Dieser habe dann sorgfältig ihre Begründetheit zu prüfen. Gebe der für die Verarbeitung Verantwortliche den Anträgen nicht statt, könne sich die betreffende Person an die Kontrollstelle oder das zuständige Gericht wenden, damit diese die erforderlichen Überprüfungen vornähmen und den Verantwortlichen entsprechend anweisen, bestimmte Maßnahmen zu ergreifen.

11.2 Neue Jugendhomepage Young Data

Medienkompetenz ist ein wesentliches Element, das junge Menschen für ihren Lebensweg benötigen, und dazu zählt in der fortschreitenden Informationsgesellschaft auch der Datenschutz. Die Enthüllungen Edward Snowdens über die anlasslosen und flächendeckenden Zugriffe auf die elektronische Kommunikation durch den US-amerikanischen Geheimdienst haben uns dies noch einmal deutlich vor Augen gehalten. Umso erfreulicher ist es, dass der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz eine neue Jugendhomepage www.Youngdata.de erstellt und Anfang 2014 freigeschaltet hat. Dort können Jugendliche, insbesondere Schülerinnen und Schüler Datenschutzkenntnisse eigenständig erwerben, sie ausbauen oder vertiefen. Diese Jugendseite soll nun als zentrale Seite der Datenschutzbeauftragten des Bundes und der Länder für den Aufbau von Datenschutzkompetenz ausgebaut werden. Für die Darstellung der Bildungsangebote im Bund und den Ländern soll ein eigener Menüpunkt „(Bildungs)angebote in Deiner Region" aufgenommen werden. Wir werden uns selbstverständlich daran beteiligen.

Daneben informierten wir die Senatorin für Bildung und Wissenschaft über dieses neue Angebot und regten an, die Schulen zu ermuntern, ihre schuleigenen Homepages mit www.Youngdata.de zu verlinken. Die senatorische Behörde teilte uns mit, bei dieser Jugendseite handele es sich in medienfachlicher Sicht um eine gelungene Homepage mit fundierten Inhalten zur Steigerung der Medienkompetenz von Schülerinnen und Schülern. Sie hat die öffentlichen Schulen und Privatschulen über die Homepage informiert.

11.3 Facebook-„Fanseiten“

Die Nutzung des sozialen Netzwerkes Facebook durch öffentliche Stellen und nicht öffentliche Stellen bleibt weiterhin nicht datenschutzkonform. Insbesondere für die öffentlichen Stellen ist die gesetzmäßige Verarbeitung von besonderen Arten personenbezogener Daten und die Wahrnehmung des Sozialgeheimnisses oder der Verschwiegenheitspflicht bei der Nutzung von Facebook-„Fanseiten“ nicht zu gewährleisten (vergleiche 36. Jahresbericht, Ziffer 12.2 sowie 35. Jahresbericht, Ziffer 11.2).

Das Verwaltungsgericht Schleswig vertrat im Oktober 2013 – für uns enttäuschend – die Auffassung, dass keine datenschutzrechtliche Mitverantwortung oder Verantwortung der Unternehmen für die Erhebung, Verwendung und Verarbeitung personenbezogener Daten von Nutzerinnen und Nutzern von „Fanseiten“ durch Facebook besteht. Diese Entscheidung wurde im September 2014 vom Oberverwaltungsgericht Schleswig bestätigt. Erst die dagegen beim Bundesverwaltungsgericht eingelegte Revision wird eine letztinstanzliche Entscheidung ergeben. In der Zwischenzeit ist aber zu beachten, dass das Verwaltungsgericht Schleswig keine Aussagen über die Rechtmäßigkeit der Facebook-„Fanseiten“ getroffen hat. Die Verwaltungen der Länder sind, worauf auch das Gericht verweist, an den Grundsatz der Gesetzmäßigkeit der Verwaltung und das Rechtsstaatsprinzip gebunden. Das bedeutet im Klartext, dass durch die nicht erwiesene Rechtmäßigkeit der sogenannten Fanseiten, also der Informationsseiten und Kommunikationsseiten bei Facebook, öffentliche Verwaltungen und andere staatliche Institutionen die Klärung dieser Rechtmäßigkeit abwarten müssen, bevor sie sich dieser Plattformen bedienen.

Dazu wird der Arbeitskreis I der Konferenz der Innenministerinnen und Innenminister des Bundes und der Länder im ersten Quartal 2015 im Auftrag der Ministerpräsidentenkonferenz Gespräche mit der Firma Facebook führen, an denen auch Vertreterinnen und Vertreter der Konferenz der Datenschutzbeauftragten des Bundes und der Länder beratend teilnehmen werden. Ziel dieser Gespräche ist es, Facebook deutlich zu machen, welche Anforderungen „Fanseiten“ erfüllen müssen, um rechtmäßig zu sein. Erst wenn diese Anforderungen erfüllt sind, wird es öffentlichen Stellen möglich sein, Facebook-„Fanseiten“ als rechtmäßige Anwendungen zu nutzen. Das Thema der großen sozialen Netze wird uns deshalb auch im Jahr 2015 weiter beschäftigen.

12. Beschäftigtendatenschutz

12.1 Öffentlicher Bereich

12.1.1 Einsatz einer elektronischen Schließanlage

Der Personalrat einer Behörde teilte mit, dort sei der Einsatz einer elektronischen Schließanlage für sämtliche Bereiche und Räume der Dienststelle geplant. Da hier in ganz erheblichem Maße personenbezogene Daten gespeichert und mit Sicherheit auch Zugangskontrollen stattfinden würden, bat der Personalrat uns mitzuteilen, worauf zu achten sei.

Wir legten dar, mit diesem System würden personenbezogene Beschäftigtendaten automatisiert verarbeitet, insbesondere über die Zugangscodes, die den bei der Behörde Beschäftigten zuzuordnen seien. Insoweit bedürfe es einer Vorabkontrolle nach dem Bremischen Datenschutzgesetz (BremDSG) im Zusammenwirken der Dienststellenleitung mit der oder dem behördlichen Datenschutzbeauftragten. Beschäftigtendaten dürfen nach dem BremDSG in Verbindung mit dem Bremischen Beamtengesetz nur verarbeitet werden, soweit dies zur Durchführung organisatorischer Maßnamen erforderlich ist und dadurch schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Regelmäßig ist es nicht erforderlich, bei elektronischen Schließanlagen zu speichern, welche Person wann welche Räumlichkeiten betreten oder verlassen hat. Bei digitalen beziehungsweise elektronischen Systemen werden immer zum Erkennen des jeweils zulässigen Codes aus tech-

nischen Gründen personenbezogene Daten automatisch gespeichert. Elektronische Schließanlagen ersetzen herkömmliche Türschlossanlagen, bei denen regelmäßig keine personenbezogenen Daten beim Öffnen und Verschließen von Türen anfallen. Der Ersatz derartiger Anlagen durch elektronische Systeme rechtfertigt jedenfalls keine Speicherung personenbezogener Beschäftigtendaten, sodass die Speicherung derartiger Daten über den für das Öffnen und Schließen einer Tür erforderlichen Zeitraum nicht erforderlich und damit unzulässig ist. Daher müssen technische und organisatorische Maßnahmen gewährleisten, dass die Daten unverzüglich nach Abschluss des Zugangs oder Verlassens der jeweiligen Räumlichkeit automatisch gelöscht werden. Dieser Aspekt ist bei der Gestaltung und Auswahl derartiger Datenverarbeitungsanlagen zu beachten.

Personalräte haben nach dem Bremischen Personalvertretungsgesetz unter anderem die Aufgabe, darüber zu wachen, dass die zugunsten der Beschäftigten bestehenden Gesetze und sonstigen Vorschriften durchgeführt werden. Dazu gehören auch die Vorschriften über den Datenschutz.

12.1.2 Fotos und Namen der Beschäftigten auf der Homepage

Beschäftigte der Bremerhavener Gesellschaft für Investitionsförderung und Stadtentwicklung (BIS) wurden gebeten, sich bei einem Fotografen Porträtfotos anfertigen zu lassen. Diese sollten auf der neuen Internetseite der städtischen Gesellschaft veröffentlicht werden. Dies entspreche einem modernen Informationsangebot, wie es viele Unternehmen seit Längerem böten. Nach uns vorliegenden E-Mails, die Erinnerungen enthielten, den Fotografen aufzusuchen, sollte dies auf freiwilliger Basis geschehen.

Wir wiesen die BIS darauf hin, dass eine derartige Einwilligung nach dem Bremischen Datenschutzgesetz nur wirksam ist, wenn sie auf der freien Entscheidung der oder des Betroffenen beruht. Hier hatten wir Zweifel, ob diese Freiwilligkeit angesichts des zu befürchtenden Gruppendrucks und der Erinnerung, den Fotografen aufzusuchen, tatsächlich gegeben war.

Eine weitere wesentliche gesetzliche Anforderung ist der Hinweis auf die Bedeutung der Einwilligung, und auf den Zweck der Datenverarbeitung, in diesem Fall der Veröffentlichung der Fotos der Beschäftigten. Gerade die Einstellung von Daten ins Internet ist problematisch, weil die Betroffenen regelmäßig nicht mehr über ihre Daten verfügen können. Auch wenn eine etwaige Einwilligung widerrufen würde, könnte die BIS die Daten allenfalls von ihrer Homepage nehmen. Die Daten blieben jedoch auf Dauer im Internet, weil Suchmaschinen darauf verlinken und diese Bilddaten jederzeit weltweit verknüpft und verwertet werden.

Auf dieses Risiko müssen die Betroffenen ausdrücklich hingewiesen werden. Außerdem ist darauf hinzuweisen, die Bilddaten jederzeit von jeder Person weltweit vielfältig mit anderen Daten auch aus sozialen Netzwerken oder sonstigen Dateien verknüpft und verfälscht werden können. Auch ein Hinweis auf die möglichen Rechtsfolgen der Verweigerung der Einwilligung und des Widerrufs einer Einwilligung mit Wirkung für die Zukunft sind erforderlich. Schließlich bedarf die Einwilligung der Schriftform, weil gerade bei einer internetbasierten Veröffentlichung von Beschäftigtendaten aus den vorgenannten Gründen ein erheblicher Eingriff in das Persönlichkeitsrecht der oder des Betroffenen gegeben ist.

Wir unterrichteten die BIS darüber, dass sie die vorgenannten Anforderungen nicht erfüllt hatte, sodass die Einwilligungen nicht wirksam waren. Dies hatte zur Folge, dass es sich um eine unzulässige Verarbeitung von Fotos der Beschäftigten handelte, sodass die Bilddaten von der Homepage der BIS gelöscht werden mussten.

Außerdem waren auf der Homepage praktisch alle Beschäftigten der BIS mit ihren vollständigen Namen (Vorname und Nachname) aufgeführt und insoweit ebenfalls weltweit

veröffentlicht worden. Hier waren ebenfalls die vorgenannten Persönlichkeitseingriffe zu befürchten.

Daraufhin erklärte die BIS, sie halte eine personalisierte Darstellung der Beschäftigten, die im Schwerpunkt eine Tätigkeit mit Außenwirkung hätten, für zwingend notwendig. Diese Personen seien erster Anlaufpunkt für die unterschiedlichen Dienstleistungen der BIS. Die Notwendigkeit werde bei der Geschäftsführung und den Bereichsleitern gesehen. Die übrigen Beschäftigten würden unter Verwendung einer den gesetzlichen Anforderungen entsprechenden Einwilligungserklärung um Einwilligung in die Veröffentlichung ihrer Daten gebeten. Sollten Beschäftigte nicht in die Veröffentlichung ihrer Daten einwilligen, würden lediglich entpersonalisierte Daten auf die Webseite gestellt. Das heißt, auf die Darstellung des Namens der oder des jeweiligen Beschäftigten werde verzichtet und die E-Mail-Adresse nicht mehr mit dem Namen sondern mit dem Aufgabenbereich gebildet. Mit diesem Ergebnis sind wir einverstanden.

12.1.3 Verlangen auf Vorlage eines begründeten Attests

Für einen Antrag auf Anerkennung der Beihilfefähigkeit für eine Heilkur verlangte die Performa Nord mittels eines Antragsformulars, dass Beamte mit Zugehörigkeit zu einer privaten Krankenversicherung ein ärztliches Attest mit ausführlicher Begründung über die Notwendigkeit der Heilmaßnahme beifügten und diesen Antrag einschließlich des ausführlichen Attestes der Beschäftigungsdienststelle vorlegten, obwohl die Beschäftigungsdienststelle in die Entscheidung über die Beihilfefähigkeit der Heilkur nicht eingebunden ist, sondern allein Performa Nord entscheidet. Nachdem wir Performa Nord um Stellungnahme gebeten hatten, wurde von dort erklärt, das Formular inzwischen so geändert zu haben, dass der Antrag nicht mehr der Beschäftigungsdienststelle vorgelegt werden muss.

12.1.4 Ausschließlich Online-Bewerbungen bei Radio Bremen

Radio Bremen verlangte, dass Bewerbungen für ein Betriebspraktikum ausschließlich über das Internet vorzunehmen seien. Laut einer Eingabe wurde in zumindest einem Fall sogar gefordert, eine Kopie des aktuellen Zeugnisses ebenfalls ausschließlich per E-Mail zu senden. Wir wiesen Radio Bremen darauf hin, dass Online-Bewerbungen regelmäßig nicht die Anforderungen des Bremischen Datenschutzgesetzes an eine sichere Übertragung teilweise sensibler Daten über Bewerberinnen und Bewerber erfüllen. Deshalb hielten wir es für erforderlich, dass Radio Bremen – auch auf seiner Homepage – zumindest ausdrücklich darauf hinweist, dass Bewerbungen einschließlich nachzureichender Unterlagen auch auf dem regulären Postweg an Radio Bremen versandt werden könnten. Daraufhin teilte die Personalleitung von Radio Bremen mit, dass sie aufgrund unserer Hinweise den Ausschreibungstext für Betriebspraktika so geändert habe, dass nunmehr Bewerbungen auch auf dem Postweg möglich seien. Damit bleibt unsere grundsätzliche datenschutzrechtliche Kritik an dem Weg der Online-Bewerbungen bestehen.

12.2 Nicht öffentlicher Bereich

12.2.1 Arbeitszeiterfassung mit biometrischen Daten

Wir erhielten den Hinweis, ein Unternehmen habe eine Arbeitszeiterfassung eingeführt, bei der die Beschäftigten mit einem Daumenabdruck Zugriff auf ihre jeweiligen Arbeitszeitkonten haben. Hierbei sei fraglich, ob der Einsatz biometrischer Daten der Beschäftigten für die Arbeitszeiterfassung erforderlich und damit zulässig sei.

Daraufhin baten wir das Unternehmen um Auskunft, ob der vorgenannte Sachverhalt zutrifft. Wir fragten insbesondere, ob und gegebenenfalls mit welchem Ergebnis vor der Entscheidung und dem Einsatz der Arbeitszeiterfassung mit biometrischen Daten eine Vorabkontrolle durch die betriebliche Beauftragte oder den betrieblichen Beauftragten für den Datenschutz erfolgt war, aus welchen Gründen sich der Arbeitgeber für das biometrische

Verfahren entschieden hatte, für welche weiteren Zwecke die biometrischen Daten genutzt würden, in welcher Weise die biometrischen Daten und die aus ihnen gewonnenen Templates beziehungsweise biometrischen Signaturen (Schablonen oder Vorlagen) auslesesicher und gegen unbefugten Zugriff geschützt seien und in welcher Weise die Beschäftigten über die technischen Systeme und die dort implementierten Verfahren, Sicherheitsvorkehrungen sowie darüber unterrichtet worden seien, wann und durch wen eine Datenerhebung und Identitätsfeststellung erfolge und für welche sonstigen Zwecke die biometrischen Daten verarbeitet oder genutzt würden.

Das Unternehmen erklärte, richtig sei, dass die Einführung eines derartigen Systems beabsichtigt sei. Für das biometrische Verfahren habe es sich aufgrund der einfachen Handhabung entschieden. Eine Vorabkontrolle sei bisher nicht erfolgt, da die Voraussetzungen hierfür nicht gesehen würden.

Daraufhin wiesen wir das Unternehmen auf die besonderen Risiken für die Rechte und Freiheiten der Betroffenen hin, die beim Einsatz körperlicher Merkmale also biometrischer Daten, wie der Daumenabdruck, vorliegen. Insbesondere die Dauerhaftigkeit erhobener und gespeicherter biometrischer Daten bedeutet, dass sie einen Menschen lebenslang charakterisieren. Auf sie kann auch nach Jahrzehnten zurückgegriffen werden. Auch wenn aus dem Daumenabdruck und Fingerabdruck weniger als aus dem Gesichtsausdruck oder der Stimme auf den körperlichen Zustand oder die psychische Verfassung der oder des Betroffenen geschlossen werden kann, sind derartige Daten hochsensibel. Mit ihnen können Informationen erhoben werden, die für den Zweck des Verfahrens nicht erforderlich sind.

Insoweit ist eine Vorabkontrolle erforderlich, für die die oder der Beauftragte für den Datenschutz zuständig ist. Dabei ist insbesondere zu untersuchen, ob es für das Unternehmen zumutbare alternative Datenverarbeitungsverfahren zur Arbeitszeiterfassung gibt, die weniger in das Persönlichkeitsrecht der Beschäftigten eingreifen als die Verarbeitung mit biometrischen Daten.

Für den Fall, dass nur ein biometrisches Verfahren eingesetzt werden könne, was zu dokumentieren wäre, seien zumindest folgende Vorgaben zur Wahrung der schutzwürdigen Interessen der Beschäftigten zu beachten: Die Speicherung und Nutzung biometrischer Daten und der aus ihnen gewonnenen Templates beziehungsweise Signaturen muss auslesesicher und gegen unbefugten Zugriff geschützt sein, die Beschäftigen müssen umfassend über die technischen Systeme und die dort implementierten Verfahren und Sicherheitsvorkehrungen und darüber unterrichtet werden, wann und durch wen eine Datenerhebung und Identitätsfeststellung erfolgt und was mit den Daten weiter geschieht.

Letztendlich erklärte das Unternehmen, davon Abstand zu nehmen, die Arbeitszeiterfassung mit biometrischen Daten einzuführen.

12.2.2 Forensische Analysen bei privater Nutzung geschäftlicher Datenverarbeitungsgeräte

Ein Arbeitgeber fragte an, ob und in welchem Umfang er befugt sei, forensische Analysen, also wissenschaftliche und technische Methoden zur Aufdeckung krimineller Handlungen der Festplatten der Datenverarbeitungsgeräte ohne Einwilligung der Beschäftigten durchzuführen. Er erlaube seinen Beschäftigen unter anderem die private E-Mail-Nutzung und Internetnutzung sowie die Speicherung privater Dateien, Spiele und Musikabspielsoftware. Wir erklärten ihm, dass derartige Analysen einen schwerwiegenden Eingriff in die Persönlichkeitsrechte seiner Beschäftigten und deshalb nur unter den Voraussetzungen des § 32 Absatz 1 Satz 2 Bundesdatenschutzgesetz zulässig wären. Danach dürfen Beschäftigtendaten zur Aufdeckung von Straftaten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die oder der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Inter-

esse der oder des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Die vorgenannte private Nutzung der geschäftlichen Datenverarbeitungsgeräte verpflichtet den Arbeitgeber, insbesondere das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme seiner Beschäftigten einzuhalten, weil hier Daten verarbeitet werden, die der privaten Lebensgestaltung der Beschäftigten zuzuordnen sind und teilweise sogar dem Fernmeldegeheimnis unterliegen. Dies schließt den Zugriff des Arbeitgebers auf private Daten seiner Beschäftigten aus. Demzufolge sollten technische und organisatorische Maßnahmen getroffen werden, die eine weitgehende Trennung der privaten und geschäftlichen Nutzung gewährleisten.

Wir haben keine Kenntnis darüber, ob es technische Systeme gibt, die forensische Analysen ermöglichen, ohne auf private Daten der Beschäftigten zuzugreifen. Selbst wenn das der Fall wäre, dürfte im Einzelfall der Einsatz derartiger Festplattenanalysen ausschließlich auf geschäftliche Beschäftigtendaten an den engen Voraussetzungen der vorgenannten Rechtsvorschrift scheitern, soweit sich die Analyse nicht ausschließlich auf den konkreten Einzelfall der Aufdeckung einer Straftat im Beschäftigungsverhältnis erstreckt. Ohne Anlass sind derartige Analysen überhaupt nicht zulässig.

12.2.3 Lastkraftwagen mit Ortungssystem

Ein Unternehmen hat seine Lastkraftwagen mit einem Ortungssystem ausgestattet, ohne dass die Beschäftigten über die konkreten Zwecke dieser Maßnahme unterrichtet wurden. Befürchtet wurde eine mehr oder weniger lückenlose Überwachung der Fahrerinnen und Fahrer, beispielsweise darüber, wann sie wie lange und wo Pausen einlegen. Auf unsere Anfrage hin erklärte das Unternehmen, die Voraussetzungen für eine Vorabkontrolle lägen nicht vor, weil keine personenbezogenen Beschäftigtendaten verarbeitet würden. Wir legten dar, dass mit der Zusammenführung der Personaleinsatzpläne und der Ortungsdaten der Fahrzeuge ein Personenbezug ohne besonderen Aufwand möglich ist. Dies erkannte das Unternehmen inzwischen an, legte seinem Beauftragten für den Datenschutz eine Verfahrensbeschreibung des Systems vor und unterrichtete die Fahrerinnen und Fahrer mit Anschreiben über die konkreten Zwecke der Datenverarbeitung.

12.2.4 Zugriffsmöglichkeit auf Personalvorgänge für alle Beschäftigten

In einer Anwaltskanzlei war nur eine Beschäftigte mit der Bearbeitung von Personalvorgängen betraut. Gleichwohl hatten alle Beschäftigten Zugriff auf die elektronisch geführten Personalvorgänge, insbesondere auf Unterlagen zu Arbeitsgerichtsprozessen. Sie konnten also Klageschriften, Klageerwiderungen in Kündigungsschutzklagen und anderen arbeitsgerichtlichen Verfahren einsehen. Diese Vorgänge enthalten sensible Personaldaten, beispielsweise zum Gehalt, die Aufzählung von Krankentagen der letzten Jahre sowie Hinweise über psychotherapeutische Behandlungen. Ebenso hatten alle Beschäftigten Zugriff auf sonstige Personalunterlagen wie Arbeitsverträge, Abmahnungen und Kündigungen.

Auf unsere Anfrage räumte die Kanzlei ein, dass die Zugriffsmöglichkeit aller Beschäftigten auf die Personalvorgänge gegen das Bundesdatenschutzgesetz verstößt und sicherte zu, die entsprechenden Personalunterlagen so zu verschlüsseln, dass ein Zugriff durch Unbefugte künftig nicht mehr möglich ist.

12.2.5 Weitergabe von persönlichen Daten durch den Arbeitgeber

Nachdem einer Augenärztin gekündigt worden war, informierte ihr Arbeitgeber ohne ihre Einwilligung eine andere Augenarztpraxis per E-Mail darüber und verband dies mit einer Bewertung der Betroffenen. Auf Anfrage erklärte der Arbeitgeber, er habe die Daten weitergegeben, um seiner Mitarbeiterin bei der Arbeitssuche zu helfen. Hierbei handelte es sich um eine unzulässige Übermittlung von Beschäftigtendaten, die eine unzulässige Daten-

speicherung beim Empfänger nach sich zog. Daher forderten wir den Arbeitgeber auf, den Empfänger der Daten aufzufordern, die personenbezogenen Daten der Betroffenen unverzüglich zu löschen und sich dies bestätigen zu lassen. Dies ist nach Angaben des Arbeitgebers inzwischen erfolgt.

12.2.6 Einsicht in ein E-Mail-Konto durch den Vorgesetzten

In einem Unternehmen, in dem die private Nutzung von E-Mail und Internet stillschweigend geduldet wurde, nahm ein Vorgesetzter Einsicht in das E-Mail-Konto eines Beschäftigten. Wir unterrichteten das Unternehmen darüber, dass aufgrund der Geltung des Fernmeldegeheimnisses nach dem Telekommunikationsgesetz nicht ohne Einwilligung der Betroffenen in E-Mail-Konten Einsicht genommen werden darf. Das Unternehmen erklärte, wegen einer längeren Abwesenheitszeit sei dies einmalig erfolgt, um feststellen zu können, ob in dieser Zeit Anfragen, Rechnungen beziehungsweise Terminabsprachen mit Lieferanten in dem Postfach aufgelaufen seien. Zukünftig würde in derartigen Fällen unverzüglich die Abwesenheitsassistenz aktiviert. Daneben würden sogenannte Teampostfächer eingerichtet. Somit sei künftig zwischen privater und betrieblicher Post einfach zu unterscheiden.

Soweit der Arbeitgeber die private E-Mail-Nutzung am Arbeitsplatz erlaubt oder stillschweigend duldet, ist er nach dem Telekommunikationsgesetz Anbieter von Telekommunikationsdiensten, wozu sowohl die Nutzung von E-Mail, Fax als auch Telefon gehören. Daraus folgt, dass der Arbeitgeber in diesen Fällen das Fernmeldegeheimnis zu achten hat. Dem Fernmeldegeheimnis unterliegen nach diesem Gesetz der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

13. Videoüberwachung

13.1 Veröffentlichung der neuen Orientierungshilfe Videoüberwachung

In den letzten Jahren ist der Bereich Videoüberwachung zu einem festen Bestandteil unserer Jahresberichte geworden. Immer häufiger wird eine Videoüberwachung eingesetzt, die sich inzwischen zu einer Technik entwickelt hat, die sich vergleichsweise kostengünstig installieren und zugleich bedienerfreundlich betreiben lässt. Neben Unternehmen und Einzelkaufleuten setzen daher immer häufiger auch Privatpersonen Kameras ein. Vielen Kamerabetreibern ist gar nicht bewusst, dass sie durch den Einsatz einer Überwachungskamera gegebenenfalls in die Rechte anderer eingreifen. Grundsätzlich hat jedoch jeder Mensch das Recht, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung zu werden. Durch eine installierte Kamera wird demgegenüber ein Überwachungsdruck erzeugt, der die Betroffenen in ihren Verhaltensweisen beeinflussen und verunsichern kann. Andererseits haben die Betreiber der Kameras diese aus einem bestimmten Grund installiert, um in der Regel ihrerseits verfassungsrechtlich geschützte Rechte wahrzunehmen. Daher wurden gesetzliche Regelungen zur Videoüberwachung geschaffen, die dem Ziel dienen, einen angemessenen Ausgleich zwischen den unterschiedlichen Interessen zu gewährleisten. Unsere Erfahrung zeigt, dass die Voraussetzungen und Grenzen unter beziehungsweise in denen eine Videoüberwachung gesetzlich erlaubt ist, häufig noch unbekannt sind. Daher wurde von den Aufsichtsbehörden des Bundes und der Länder eine gemeinsame Orientierungshilfe für den zulässigen Einsatz von Videokameras erarbeitet und veröffentlicht (https://ssl.bremen.de/datenschutz/sixcms/media.php/13/Orientierungshilfe%20Video%FCberwachung%20durch%20nicht-%F6ffentliche%20Stellen.pdf). Das Ziel dieser Orientierungshilfe ist es, den für die Videoüberwachung Verantwortlichen konkrete Hinweise für ihre eigenverantwortliche Prüfung zu geben und den von der Überwachung Betroffe-

nen die gesetzlichen Vorgaben zu erläutern, damit sie erkennen können, ob sie eine Videoüberwachung hinzunehmen haben oder sich dagegen wehren können. Darüber hinaus bleibt zu hoffen, dass es durch die Veröffentlichung gelingt, die Sensibilität hinsichtlich der Nutzung von Videokameras zu erhöhen.

13.2 Justizvollzugsanstalt

In diesem Berichtsjahr begleiteten wir die Einführung einer Videoüberwachungsanlage in der Justizvollzugsanstalt Bremen weiter (vergleiche 36. Jahresbericht, Ziffer 6.2 und 35. Jahresbericht, Ziffer 6.2). Wir besichtigten die Anlage vor Ort und stellten dabei einige datenschutzrechtliche Mängel fest. So wiesen beispielsweise verschiedene Kameras im Außenbereich keine ausreichende Begrenzung des Zoombereichs und Schwenkbereichs auf. Die Einrichtung einer solchen Sperre verhindert auf technischem Wege, dass Bereiche von der Kamera erfasst werden, die aus rechtlichen Gründen nicht überwacht werden dürfen. Was die Videobeobachtung des Innenbereiches der Anstalt anbelangt, kritisierten wir beispielsweise das Filmen des Zeiterfassungsgeräts, das durch die Bediensteten genutzt wird. Einige der Kameraeinstellungen wurden in der Zwischenzeit korrigiert. Bei den anderen äußerte die Leitung der Justizvollzugsanstalt Sicherheitsbedenken, die der Änderung des Erfassungswinkels entgegenstünden. Wir werden die noch offenen Punkte unter Berücksichtigung der Stellungnahme der Anstaltsleitung erneut kontrollieren.

Bei dem zugehörigen Datenschutzkonzept sehen wir Änderungsbedarf beziehungsweise Ergänzungsbedarf insbesondere bei den Fristen für das Sperren und Löschen der Daten sowie beim Fernwartungskonzept und Berechtigungskonzept. Eine Antwort der Justizvollzugsanstalt zu unserer Stellungnahme steht noch aus.

Im letzten Jahresbericht (vergleiche 36. Jahresbericht, Ziffer 6.2) hatten wir bemängelt, dass für die Videoüberwachung in der Justizvollzugsanstalt keine hinreichende Rechtsgrundlage besteht. Hinsichtlich dieses Punktes bestand ein Dissens mit dem Senator für Justiz und Verfassung, der die einschlägigen Vorschriften im Untersuchungshaftvollzugsgesetz als ausreichend angesehen hatte. Dieser Streitpunkt ist jetzt insofern obsolet, als in den Entwurf eines Bremischen Strafvollzugsgesetzes eine Vorschrift zur Videoüberwachung mit aufgenommen wurde.

13.3 Eigensicherung der Polizeien

Über das Verfahren zur Videoaufzeichnung in Polizeifahrzeugen zum Zweck der Eigensicherung gemäß § 29 Absatz 5 Bremisches Polizeigesetz berichteten wir bereits (vergleiche 35. Jahresbericht, Ziffer 5.8 und 30. Jahresbericht, Ziffer 9.1). Aufgezeichnet wird das Vorgehen der Polizeibeamtinnen und Polizeibeamten bei Anhaltevorgängen und Kontrollvorgängen im öffentlichen Verkehrsraum.

Im vergangenen Berichtsjahr ließen wir uns das bestehende Verfahren bei der Polizei Bremen vor Ort an einem Fahrzeug beispielhaft zeigen und verglichen die weitere Datenverarbeitung mit der bestehenden Datenschutzdokumentation. Dabei stellten wir Abweichungen zur vorliegenden Verfahrensbeschreibung fest. Wir nahmen zu den einzelnen Punkten Stellung und übermittelten der Polizei Bremen unsere Hinweise zum Datenschutz. Trotz Nachfragen wurde uns in diesem Berichtsjahr keine aktualisierte Verfahrensbeschreibung vorgelegt, sodass unklar ist, ob unsere Hinweise zur Verfahrensgestaltung umgesetzt worden sind.

Weiterhin nahmen wir in diesem Berichtsjahr das Verfahren bei der Ortspolizeibehörde Bremerhaven in Augenschein und wiesen darauf hin, dass die vorliegende Verfahrensbeschreibung zu ergänzen ist. Außerdem halten wir es für erforderlich, die Mitarbeiterinnen und Mitarbeiter, die das System zur Videoaufzeichnung in den Fahrzeugen bedienen,

regelmäßig daran zu erinnern, dass die betroffenen Bürgerinnen und Bürger über die Aufzeichnung informiert werden müssen.

13.4 Lehrerausbildung

Eine Schule wies uns darauf hin, dass von Lehramtsstudierenden der Universität Bremen nach dem „Handbuch schulpraktische Studien“ verlangt wird, die Videografie einer Unterrichtsstunde anzufertigen. Praktisch gleichzeitig fragte uns die Universität Bremen, ob ein Videoeinsatz im Schulunterricht zulässig sei, wenn bei einer Verweigerung der Einwilligung durch die Erziehungsberechtigen deren Kinder nicht auf der Videoaufnahme zu sehen seien.

Beachtlich ist in diesem Zusammenhang, dass audiovisuelle Aufnahmen besondere Auffälligkeiten, auch nur geringe Gehdefizite oder Sprachdefizite beziehungsweise Ausdrucksdefizite der Studierenden sowie der Schülerinnen und Schüler registrieren und speichern. Ein solcher Eingriff in die Persönlichkeitsrechte am eigenen Bild und am gesprochenen Wort wäre ohne wirksame Einwilligungen nur zulässig, wenn eine den Anforderungen der Normenklarheit, Verhältnismäßigkeit und Zweckbindung entsprechende Rechtsvorschrift dies ausdrücklich erlaubte. Die Regelung im Handbuch ist keine derartige Rechtsgrundlage. Daher könnten solche Aufnahmen allenfalls durch Einwilligungen gerechtfertigt werden.

Was die Anfrage nach dem Verzicht auf Videoaufnahmen von Schülerinnen und Schülern anbelangt, deren Erziehungsberechtigte keine Einwilligung erteilt haben, erklärten wir, auch wenn Personen nicht auf der Videoaufnahme zu sehen seien, würden deren Wortbeiträge oder sonstige Tonbeiträge aufgenommen, was ebenfalls einer Einwilligung bedürfte. Darüber hinaus haben wir erhebliche Zweifel, ob die Einwilligungen der Eltern und Lehramtsstudierende in solchen Videoaufnahmen überhaupt wirksam sein können. Nach unseren Erfahrungen mit Eingaben von Eltern im Schulbetrieb befürchten nämlich viele, dass ihre Kinder im Unterricht benachteiligt werden, sollten Einwilligungen verweigert werden. Das Gleiche gilt für Lehramtsstudierende, die bei Verweigerung der Einwilligung schlechtere Benotungen befürchten. In solchen Fällen fehlt es an der Freiwilligkeit und damit der Rechtswirksamkeit der Einwilligungserklärungen. Sollten Videografien ohne wirksame Einwilligung angefertigt worden sein, wären sie nach dem Bremischen Datenschutzgesetz zu löschen.

Die Universität Bremen erklärte dazu, das entsprechende Modul sei aus dem Handbuch entfernt worden. Darüber hinaus habe sie die zuständigen Hochschullehrenden darauf hingewiesen, dass Videografien, die ohne Einwilligung der Eltern stattgefunden hätten, zu löschen seien. Darüber hinaus erklärte sie, um entstandene Irritationen und Unsicherheiten auszuräumen und ein datenschutzrechtlich sicheres Verfahren zu erreichen, werde für diese Problematik ein Gespräch mit dem Bildungsressort anberaumt; unsere Teilnahme daran werde dabei als hilfreich angesehen. Nach Angaben der Universität Bremen fand zwischenzeitlich eine derartige Besprechung statt, zu der wir nicht eingeladen wurden. Dabei sei festgelegt worden, dass die Durchführung von Videografien unter Einhaltung der datenschutzrechtlichen Bestimmungen zu erfolgen habe. Vereinbart worden sei, dass eine von allen Hochschullehrenden im Lehramtsstudium zu verwendende, den Datenschutzanforderungen entsprechende, Einwilligungserklärung erstellt und uns zur Prüfung vorgelegt werden solle.

Inzwischen legte die Universität ein Muster einer Einwilligungserklärung der Erziehungsberechtigten vor, das jedoch die gesetzlichen Anforderungen noch nicht erfüllte. So fehlte eine Aufklärung darüber, dass die Videografien auch an Prüferinnen und Prüfer der Lehrerausbildung übermittelt werden. Auch der Hinweis, dass die Ansprache von Schülerinnen und Schülern mit Vornamen sowie mögliche Auswirkungen auf das Klassenverhalten und die Reaktionen der Schülerinnen und Schüler festgehalten werden, ist keine angemessene Aufklärung. Hinsichtlich der Rechtsfolgen bei einer Verweigerung der Einwilligung oder einem Widerruf mit Wirkung für die Zukunft bedarf es noch einer ausdrücklichen Aufklä-

rung darüber, dass die Möglichkeit besteht, dass das Kind nicht an einem videografierten Unterricht teilnimmt.

Wir baten die Universität, diese Problematik mit der Senatorin für Bildung und Wissenschaft zu klären. Hierzu boten wir unsere Mitwirkung an.

Die Übersendung des Musters für eine Erklärung, mit der die Lehramtsstudierenden einwilligen, sich im Unterricht videografieren zu lassen und sich damit einverstanden erklären, dass die Aufnahmen von Prüferinnen und Prüfern der Universität ausgewertet werden, steht noch aus.

13.5 Visite im Krankenzimmer

Ein Krankenhaus informierte uns darüber, dass ein Mitpatient in einem Krankenzimmer eine Visite möglicherweise mit einem Smartphone aufgenommen habe. Dieser Hinweis ging nach Angaben des Krankenhauses erst nach Entlassung dieses Patienten ein. Es bestehe die Vermutung, dass vertrauliche und sensible Informationen in Wort und Bild aufgenommen worden seien. Die Aufnahmen betreffen zwei Patienten sowie zwei Ärztinnen und eine Pflegekraft, die während der Visite im Zimmer anwesend waren. Wir rieten dem Krankenhaus, den Patienten, dem die Videoaufnahme vorgeworfen wird, aufzufordern, das Video zu löschen und Personen, an die er das Video weitergeleitet habe, zur Löschung des Videos aufzufordern und dies dem Krankenhaus zu bestätigen. Die Mitpatienten und die betroffenen Mitarbeiterinnen wurden darüber informiert, dass sie rechtliche Schritte gegen den videografierenden Patienten einleiten können.

13.6 Videoüberwachung von Beschäftigten

Wir hatten wieder eine Vielzahl von Eingaben, die sich gegen Videoüberwachungen von Beschäftigten wandten, insbesondere weil deren Arbeitsplätze mehr oder weniger lückenlos im Visier von Kameras waren. Beispielhaft berichten wir über drei Fälle:

Einmal handelte es sich um ein Möbelgeschäft, in dem gezielt der Tischbereich im Verkaufsraum, an dem Beratungen mit Kundinnen und Kunden stattfinden sowie der Kassenbereich erfasst wurden. Hier setzten wir durch, dass diese Bereiche nicht mehr erfasst werden, weil dort die genannten Zwecke Verhinderung von Ladendiebstahl und Vandalismus regelmäßig nicht erreicht werden können.

In einem weiteren Fall waren die Kameras in einer Werkhalle auf die Arbeitsplätze ausgerichtet. Dies wurde mit der Notwendigkeit zur Verhinderung von Diebstahl und mit Anforderungen der Versicherung begründet. Auch hier setzten wir durch, dass die Kameras nicht mehr die Arbeitsplätze erfassen, sondern so ausgerichtet werden, dass nur die unmittelbaren Toreingänge der Werkhalle überwacht werden.

Ein anderer Fall betraf eine Lagerhalle, in der ein besonders zu sichernder Bereich videoüberwacht wurde. Dort werden Zigarettenpaletten gelagert und zum Weitertransport auf Lastkraftwagen verbracht. Hierzu sieht eine Betriebsvereinbarung vor, dass in diesem Bereich die Videoüberwachung automatisch ausgeschaltet wird, wenn sich während der regulären Arbeitszeit Beschäftigte der Firma mit einer speziellen Zugangsmöglichkeit dort aufhalten. Diese Ausschaltfunktion war nicht aktiviert, sodass die Beschäftigten dort unzulässig videoüberwacht wurden. Wir erreichten, dass die Videoüberwachung in diesem Bereich den Vorgaben der Betriebsvereinbarung angepasst wurde.

In den meisten bearbeiteten Fällen mangelte es an angemessenen Unterrichtungen der Beschäftigten über die Videoüberwachung, ausreichenden Hinweisschildern sowie eindeutigen Verfahrensbeschreibungen einschließlich klarer Regelungen über den Anlass und den Zugriff auf die Videodaten sowie deren Protokollierung.

13.7 Fußballplatz

Im Juli des Berichtsjahres wurde an uns aus dem Ausschuss für Wissenschaft, Medien, Datenschutz und Informationsfreiheit der Bremischen Bürgerschaft eine Berichtsbitte herangetragen. Sie bezog sich auf die Videoüberwachung eines Fußballplatzes in Bremen. Da uns die vorgetragene Videoüberwachungsmaßnahme nicht bekannt gewesen war, schrieben wir umgehend die verantwortliche Stelle per Fax an und baten um kurzfristige Stellungnahme. Der anschließende Schriftwechsel führte zu einem Vorortttermin mit der verantwortlichen Stelle. Bei der Vorortbesichtigung verdeutlichten wir der verantwortlichen Stelle, welche Kamerastandorte und Erfassungsbereiche datenschutzrechtlich zulässig sind, dass eine Überwachung nur außerhalb des zeitlich festgelegten Spielbetriebes durchgeführt werden darf und dass dieser Umstand aus dem Hinweisschild zur Videoüberwachung hervorgehen muss. Inzwischen wurde uns von der verantwortlichen Stelle die Umsetzung der von uns geforderten Maßnahmen bestätigt.

13.8 Restaurantkette

Ein Petent beschwerte sich bei uns über diverse Überwachungskameras, die im Innenbereich einer Filiale einer großen Restaurantkette installiert seien. Er fühle sich beim Essen beobachtet, weil auch die Sitzbereiche überwacht würden. Nachdem wir bei der Geschäftsführung angefragt hatten, wurde uns bestätigt, dass in fast allen Filialen der Kette Überwachungskameras installiert seien. Aufgrund dieser Stellungnahme vereinbarten wir umgehend einen Prüftermin, um in Anwesenheit der Geschäftsführung sowie des betrieblichen Datenschutzbeauftragten die Angelegenheit in Augenschein zu nehmen. Bei der Vorortbesichtigung von zwei Filialen konnten wir feststellen, dass der Erfassungsbereich einiger Kameras auch auf die Sitzbereiche ausgerichtet war. Wir teilten der verantwortlichen Stelle mit, welche Kamerastandorte datenschutzkonform wären und sprachen deren Erfassungsbereiche ab. Dabei erzielten wir mit den Vertretern der Restaurantkette Einigkeit darüber, dass die getroffenen Absprachen auch auf derzeit deaktivierte Kameras zu übertragen sind. Die Vertreter der verantwortlichen Stelle stimmten uns darin zu, dass bei den Betroffenen auch durch solche Kameras optisch der Eindruck erweckt wird, es handele sich um eine funktionstüchtige Kamera, bei der ständig mit einer überwachenden Aufzeichnung zu rechnen sei. Uns wurde zugesichert, dass die abgesprochenen und vereinbarten Kriterien zu den zulässigen Standorten der installierten Kameras auch auf alle übrigen Filialen im Land Bremen übertragen und dort jeweils umgesetzt werden.

13.9 Café

Eine Besucherin eines Cafés teilte uns mit, dass dort Überwachungskameras installiert seien. Hierdurch fühle sie sich in ihren Bürgerrechten verletzt. Auf unsere schriftliche Anfrage hin bestätigte uns der Geschäftsinhaber des Cafés die Installation von insgesamt vier Kameras, die rund um die Uhr aufzeichneten. Die Kameras seien installiert worden, weil sich das Café in einem besonders einbruchsgefährdeten Stadtteil befinde. Bei einer Vorortbesichtigung stellten wir fest, dass durch die Kameras sowohl die Sitzbereiche im Café als auch die beidseitigen Verkaufstresen mit erfasst wurden. Daraufhin erläuterten wir dem Besitzer die rechtlichen Voraussetzungen zur Videoüberwachung eingehend. Wir konnten ihn davon überzeugen, dass die derzeitigen Kamerapositionen sowie Erfassungsbereiche nicht in seinem Geschäftsinteresse lagen, da sich auch seine anderen Gäste wie die Petentin dadurch möglicherweise beobachtet fühlten und letztlich das Café aus diesem Grund vielleicht nicht wieder besuchten. Anschließend teilten wir ihm mit, welche Maßnahmen von ihm umzusetzen waren, um die Überwachung mit den gesetzlichen Anforderungen an den Datenschutz in Einklang zu bringen. Der Geschäftsinhaber bestätigte uns später, dass die Kameras unseren Forderungen entsprechend an den mit uns abgesprochenen Standorten montiert worden seien und die Kameras nur außerhalb der Geschäftszeiten aktiviert würden. Ebenso seien eine Verfahrenbeschreibung erstellt und deutlich sichtbare Hinweisschilder an den abgesprochenen Stellen angebracht worden.

13.10 Flugdrohnen

Flugdrohnen werden in Deutschland als neue Maßnahme der Polizei zur Gefahrenabwehr eingesetzt, was im Arbeitskreis Sicherheit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder thematisiert wurde. Die Polizeien im Land Bremen setzen derzeit keine Flugdrohnen ein. Mittels Videokameras an Fluggeräten werden Menschen aus der Luft überwacht. Im Vergleich zu den üblichen, fest installierten Videokameras und zu den mobilen Videokameras, die etwa in Polizeifahrzeugen mitgeführt werden, ergeben sich daraus zwei Unterschiede: der Blickwinkel und die Erkennbarkeit für die Betroffenen. Die Beobachtung aus der Luft erlaubt anders als die Beobachtung vom Boden die Überwindung von Hindernissen, die gegen unerwünschte Einblicke errichtet worden sind. So sind aus der Luft Einblicke in private Bereiche wie Gärten, Hinterhöfe oder durch die Fenster in Wohnungen problemlos möglich. Auch die Größe, die Brennweite oder der Lärm der Flugdrohnen führen nicht immer dazu, dass betroffene Personen diese Fluggeräte wahrnehmen, sodass die Videokamera, der beobachtete Bereich, die verantwortliche Stelle oder der Zweck der polizeilichen Maßnahme nicht ohne Weiteres erkennbar sind. Nach den gesetzlichen Grundlagen für die optisch-elektronische Überwachung muss die oder der Betroffene aber vor dem Betreten des überwachten Bereichs den Umstand der Beobachtung erkennen können, da sie oder er einschätzen können muss, welcher Bereich von einer Videokamera erfasst wird und damit in die Lage versetzt wird, der Überwachung ausweichen oder sein Verhalten anpassen zu können. Die Erkennbarkeit der verantwortlichen Stelle ist bedeutsam für die Feststellung, an wen sich die betroffene Person zur Wahrung ihrer Rechte wenden kann. Der Einsatz von Flugdrohnen durch die Polizei stellt aufgrund dieser neuen Qualität einen tiefgreifenden Eingriff in das Recht auf informationelle Selbstbestimmung dar. Er ist gegenwärtig nicht von einer gesetzlichen Grundlage gedeckt.

13.11 Schwerpunktbereiche im Laufe des Jahres

Auch in diesem Berichtsjahr erhielten wir zahlreiche Anfragen und Beschwerden zur Videoüberwachung öffentlicher Fußwege, Straßen sowie Parkplätze. Hierbei handelte es sich vorwiegend um Fälle, in denen die Betreiber der Kameras ihr Eigentum vor Vandalismus schützen wollten, wobei jedoch durch die Ausrichtung der Kameras auch immer öffentliche Bereiche mit erfasst wurden.

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

In vielen Fällen der Überwachung von Hausfassaden stützen sich die Betreiber der Anlagen auf die Wahrnehmung des Hausrechts. Dieses rechtfertigt es jedoch nicht, öffentliche Straßen, Wege und Parkplätze mit zu erfassen. Eine Überwachung der Hausfassaden ist grundsätzlich nur zulässig, wenn dabei nicht auch öffentlich zugängliche Bereiche erfasst werden. Sollte dies jedoch nicht vermieden werden können, weil etwa die Hausfassade direkt an einen Fußweg angrenzt, darf die Überwachung nur auf das zwingend notwendige Ausmaß beschränkt werden und einen maximal einen Meter breiten Streifen entlang der Fassade erfassen. Voraussetzung ist allerdings, dass es sich nachweislich um einen besonders einbruchsgefährdeten oder beschädigungsgefährdeten Bereich handelt.

Andere Betreiber rechtfertigten den Betrieb ihrer Kamera damit, dass sie diese zur Wahrnehmung berechtigter Interessen installiert hätten. Es handelte sich zumeist um Fälle, in denen durch die im Haus oder in der Wohnung installierten Kameras öffentliche Parkplätze, Parkbuchten am Straßenrand oder der Randstreifen der Straße überwacht wurden. Die Betreiber wollten durch die Überwachungsmaßnahme ihr dort geparktes Auto vor Übergriffen schützen und die gespeicherten Aufnahmen als Beweismittel für Strafanzeigen

verwenden. Bei der Wahrnehmung berechtigter Interessen handelt es sich nach dem Willen des Gesetzgebers um einen eng auszulegenden Ausnahmetatbestand. Die geschilderten generalpräventiven Maßnahmen und die Erleichterung der Strafverfolgung sind nicht Aufgabe von Privatpersonen, sondern den Strafverfolgungsbehörden vorbehalten. Würden derartige Überwachungsmaßnahmen als berechtigtes Interesse der Privatpersonen anerkannt werden, wäre es praktisch jeder Person gestattet, eine Überwachung und Identifizierung verdächtiger Personen, die sich auf öffentlichen Straßen und Wegen aufhalten, durchzuführen. Die Folge könnte eine Totalüberwachung sein, was jedoch nicht mit der vom Gesetzgeber beabsichtigten begrenzenden Wirkung des § 6b BDSG zu vereinbaren wäre.

Um in den angesprochenen Bereichen einer ausufernden Videoüberwachung entschieden entgegenzuwirken, wird uns dieses Aufgabenfeld sicherlich auch zukünftig weiterhin stark in Anspruch nehmen und eine stete Herausforderung für uns darstellen.

14. Auskunfteien

14.1 Scoring bei Wirtschaftsauskunfteien oder: Die Schwierigkeit treffsicherer Zukunftsprognosen

Bereits in unserem 32. Jahresbericht hatten wir ausführlich über die Fragwürdigkeit sogenannter Scoringverfahren bei Wirtschaftsauskunfteien berichtet (siehe dort Ziffer 13.6.4).

Scoringverfahren ermöglichen nach den Anpreisungen der Wirtschaftsauskunfteien das Treffen von Vorhersagen zum künftigen Zahlungsverhalten beziehungsweise zur künftigen Zahlungsausfallwahrscheinlichkeit einer bestimmten Person. Jede Wirtschaftsauskunftei setzt auf eigene Scoringverfahren. Der im Scoringverfahren ermittelte Scorewert für ein und dieselbe Person kann daher bei unterschiedlichen Auskunfteien völlig unterschiedlich ausfallen. Der Scorewert wird dabei regelmäßig in Form eines mathematisch-statistischen Wahrscheinlichkeitswertes angegeben. Statistische Zahlen wirken objektiv und verlässlich. Aber ob statistische Zahlenwerte tatsächlich ein wahres, verlässliches Bild der Verhältnisse abgeben, hängt neben der eingesetzten Berechnungsformel maßgeblich von der Korrektheit der verwendeten Datenbasis ab. Die Berechnungsformel betrachten die Auskunfteien als Betriebsgeheimnis. Allerdings verrät bereits ein Blick auf die Datenbasis bei Auskunfteien viel über die Werthaltigkeit und Verlässlichkeit ihrer Prognosen: Auskunfteien haben keine Kenntnis über (sicheres) monatliches Einkommen der zu beurteilenden Person und ihre monatlichen finanziellen Gesamtbelastungen, also zwei Basismerkmale für die verlässliche Beurteilung der Zahlungsfähigkeit einer Person. Zudem sind bei Auskunfteien oftmals insgesamt nur sehr wenige Informationen zu Personen gespeichert und die gespeicherten Daten oftmals falsch oder veraltet, wie eine umfassende Untersuchung bereits im Jahr 2009 ans Licht förderte. Schließlich haben nicht wenige der den Auskunfteien verfügbaren Daten beziehungsweise Informationen zum individuellen Wirtschaftsverhalten ohne ihren Kontext keinen eindeutigen Aussagegehalt. So bedeutet etwa das Fehlen von Informationen zu Bankkrediten nicht zwingend, dass diese Personen besonders liquide sind. Es kann vielmehr auch schlicht Resultat einer bislang äußerst sparsamen Lebensführung oder gegebenenfalls privat erhaltener oder der Auskunftei nicht bekannt gewordener kreditwirtschaftlicher Darlehen sein. Dass eine Person eine Forderungssumme nicht bezahlt, kann an Geldmangel aber ebenso gut daran liegen, dass die Geltendmachung der Forderung unberechtigt ist, die Person rechtlich nichts schuldet.

Zu diesen statistischen Problemen kommt eine grundsätzliche Problematik hinzu, die für alle Versuche eines vorausschauenden Blicks in die Zukunft gilt und die bereits vor über zweihundert Jahren Friedrich Schiller trefflich wie folgt beschrieb: „Nichts Wahres lässt sich von der Zukunft sagen.“ Oder mit Mark Twain gesprochen: „Prognosen sind schwierig, insbesondere wenn sie die Zukunft betreffen.“

Gerade in dem Lebensbereich, den Scoringverfahren einer Bewertung zugänglich machen wollen, nämlich der Zahlungsausfallwahrscheinlichkeit einer bestimmten natürlichen Person in einem längeren zukünftigen Zeitraum, spielen eben zahlreiche unberechenbare Variablen eine Rolle. Ein plötzlicher Arbeitsplatzverlust etwa katapultiert die individuelle Zahlungsausfallwahrscheinlichkeit von einem Moment auf den anderen schlagartig in die Höhe. Mit anderen Worten: Die Zukunft entwickelt sich eben regelmäßig nicht einfach linear zur Vergangenheit. Die Grundannahme einer linearen Entwicklung liegt aber – vereinfacht gesagt – den Scoringverfahren zugrunde. Denn die Referenzdaten der Auskunfteien bestehen eben nur aus mehr oder weniger umfangreichen Informationen zum sektoralen Zahlungsverhalten einer mehr oder wenigen großen Vergleichsgruppe von Personen aus einer mehr oder weniger fernen Vergangenheit. Diese mehr oder weniger umfangreichen Zahlungserfahrungswerte der Vergangenheit einer möglicherweise nicht repräsentativen Personengruppe werden nun – vereinfachend gesagt – auf die zu bewertende Vergleichsperson übertragen und sollen bei dieser nun die individuelle Zahlungsausfallwahrscheinlichkeit in der Zukunft beschreiben.

Nach alledem verwundert es wenig, dass bereits im Jahr 2009 eine im Auftrag des Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz erstellte Studie im Wesentlichen zu dem Ergebnis kam, dass das Zustandekommen von Scorewerten bei Auskunfteien nicht nachvollziehbar und die Aussagekraft von Scorewerten äußerst zweifelhaft sei. Bereits ein Jahr zuvor hatte eine im Auftrag der Verbraucherzentrale Bundesverband e. V. erstellte Studie dem Scoring der Auskunfteien bescheinigt, für eine verlässliche Beurteilung der Bonität von Verbraucherinnen und Verbrauchern kaum tauglich zu sein.

Ungeachtet aller tatsächlichen Probleme der Scoringverfahren bei Auskunfteien fügte der Bundesgesetzgeber auf Basis eines Entwurfs des Bundesministeriums des Innern mit Wirkung zum 1. April 2010 eine Rechtsvorschrift in das Bundesdatenschutzgesetz ein, die allgemeine Zulässigkeitsvoraussetzungen für das Scoring festlegen sollte. Von Anfang an zeichnete sich ab, dass diese Rechtsvorschrift keine effektiven – und zudem kaum zuverlässig nachkontrollierbaren – Zulässigkeitsvoraussetzungen an Scoringverfahren aufgestellt und schutzwürdige Interessen des Einzelnen vor Reduzierung seiner Person auf einen automatisiert ermittelten, intransparenten Zahlenwert weitestgehend ignoriert hatte.

Das Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz führte sodann im Sommer des Jahres 2012 eine Umfrage zu den Erfahrungen der Länder beziehungsweise ihrer Datenschutzaufsichtsbehörden mit der neuen Scoring-Rechtsvorschrift durch. Das Resultat spiegelte sich in zahlreichen Presseberichten über die Zweifelhaftigkeit der gesetzlichen Regelung des Scoringverfahrens und die Fragwürdigkeit der praktizierten Auskunfteien-Scoringverfahren wieder.

Zu Beginn des Jahres 2013 schrieb das Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz zusätzlich einen Auftrag zu einer wissenschaftlichen Studie mit dem Gegenstand „Scoring nach der Datenschutznovelle 2009 und neue Entwicklungen“ aus, in deren Zuge insbesondere also die Auswirkungen der seit 2010 geltenden Scoringvorschrift des Bundesdatenschutzgesetzes eingehender untersucht werden sollten. Nachdem mit Beginn der neuen Legislaturperiode die Geschäftsverteilung der Bundesregierung geändert und der Verbraucherschutzbereich in den Geschäftsbereich des Bundesjustizministeriums übergegangen war, zeichnet dieses nunmehr für die Scoring-Studie verantwortlich.

Das umfangreiche Gutachten wurde gegen Ende des Berichtsjahres dem nunmehr zuständigen Bundesministeriums der Justiz und für Verbraucherschutz vorgelegt, dort aber zunächst unter Verschluss gehalten. Laut Presseberichten war dies darauf zurückzuführen, dass es mit dem Bundesministerium des Innern, in dessen Geschäftsbereich grundsätzlich die Zuständigkeit für das Datenschutzrecht angesiedelt ist, Unstimmigkeiten hinsichtlich etwaig gesetzgeberisch zu ziehender Konsequenzen gab. Es wäre nicht das erste Mal, dass das Bundesministerium des Innern Bemühungen zur Schaffung effektiver Regelun-

gen zum Persönlichkeitsrechtsschutz des einzelnen Bürgers trotz offensichtlich bestehender Notwendigkeiten blockiert, unter Hinweis auf die europäischen Bemühungen um eine Datenschutzgrundverordnung hinhält oder lediglich Alibi-Aktivitäten entfaltet. Exemplarisch sei nur an die verunglückte Novellierung der datenschutzrechtlichen Werbevorschriften im Bundesdatenschutzgesetz, die langjährige Verzögerung der Schaffung von Arbeitnehmerdatenschutzvorschriften, die ihren Namen verdienen, die bis vor kurzem standhafte Nichtumsetzung eines Urteils des Europäischen Gerichtshofs zur Unabhängigkeit der Datenschutzaufsicht im Hinblick auf den beziehungsweise die Bundesdatenschutzbeauftragte trotz offensichtlicher Übertragbarkeit des Urteils auf die Bundesebene, die Zulassung des sogenannten Geoscorings trotz aller geäußerter Bedenken an der Ermöglichung einer solchen statistischen Wohnumfeldhaftung, die Nichtumsetzung eines Handlungsauftrags des Petitionsausschusses des Deutschen Bundestages zur Novellierung der Löschungsprüffristen im Bundesdatenschutzgesetz (siehe Ziffer 14.2 dieses Berichts) erinnert. Die Liste ließe sich erweitern. Auf den Seiten des Bundesministeriums der Justiz und für Verbraucherschutz ist die Studie nunmehr aber für jedermann abrufbar (http://www.bmjv.de/SharedDocs/Kurzmeldungen/DE/2014/20141215-Scoring-Studie.html?nn=3433226).

14.2 Nichtumsetzung eines Urteils des Europäischen Gerichtshofs zum Umfang der Betroffenenrechte im Bundesdatenschutzgesetz

Bereits im Mai 2009 hatte der Europäische Gerichtshof in der Rechtssache C-553/07 entschieden, dass das Auskunftsrecht der von einer Datenverarbeitung Betroffenen aus Artikel 12 Buchstabe a der europäischen Datenschutzrichtlinie auch ein Recht der Betroffenen auf Auskunft über den Inhalt der übermittelten Daten umfasst. Der deutschen Umsetzungsvorschrift zu diesem Artikel der Datenschutzrichtlinie, dem § 34 Bundesdatenschutzgesetz, ist dies im Wortlaut jedoch nicht zu entnehmen. Diese Regelungslücke lässt sich auch im Wege der Gesetzesauslegung nicht beseitigen. Auch eine direkte Berufung einer beziehungsweise eines Betroffenen auf das weitergehende Auskunftsrecht der europäischen Richtlinienvorschrift zulasten einer auskunftspflichtigen Stelle ist nach Rechtsprechung des Europäischen Gerichtshofs nicht möglich.

Auf die daher bestehende Notwendigkeit einer Umsetzung des Urteils des Europäischen Gerichtshofs im Bundesdatenschutzgesetz hatten die Datenschutzaufsichtsbehörden mehrheitlich bereits im Herbst 2009 das zuständige Bundesministerium des Innern aufmerksam gemacht. Eine Umsetzung hat jedoch selbst fünf Jahre nach Ergehen des Urteils nicht stattgefunden. Bewusst wird damit also eine europarechtswidrige Verkürzung der Rechtsposition Betroffener über mehrere Jahre hinweg in Kauf genommen.

Die kritikwürdige Tendenz der Bundesregierung, selbst dringend notwendige Änderungen des Bundesdatenschutzgesetzes auf den Sankt-Nimmerleins-Tag hinauszuschieben, zeigt sich auch an dem Schicksal einer Empfehlung des Petitionsausschusses des Deutschen Bundestages aus dem Frühjahr 2012. Der Petitionsausschuss hatte eine Neuregelung der Prüffrist für die Löschung bonitätsbezogener Daten bei Wirtschaftsauskunfteien empfohlen. Nach der bestehenden Regelung beginnt nämlich die dreijährige beziehungsweise vierjährige Frist, nach deren Ablauf die Notwendigkeit einer weiteren Speicherung von Bonitätsmerkmalen durch Wirtschaftsauskunfteien automatisch zu prüfen ist, erst mit dem 1. Januar des der Merkmalsspeicherung folgenden Kalenderjahres. Dies hat zur Konsequenz, dass bei zwei Schuldnern mit einem etwa zur gleichen Zeit entstandenen und inhaltlich vergleichbaren Negativmerkmal eine unterschiedliche Prüffristlänge gelten kann, je nachdem wann zufälligerweise das Negativmerkmal gespeichert wurde. Wurde das Negativmerkmal nämlich bei Schuldner X am 31. Dezember 2012 gespeichert, bei Schuldner Y zufällig erst zwei Tage später, also am 2. Januar 2013, so beginnt der Prüffristlauf für Schuldner X bereits am 1. Januar 2013, für Schuldner Y erst am 1. Januar 2014. Im Ergebnis muss damit Schuldner Y eine fast um ein Jahr längere Speicherung hinnehmen, obwohl es sich um ein zur gleichen Zeit entstandenes und inhaltlich gleiches Negativmerkmal handelt. Er hatte schlicht Pech, dass die Speicherung des Negativmerkmals bei ihm erst zu Beginn des Jahres 2013 erfolgte. Diese Ungleichbehandlung lässt sich vor dem

Hintergrund des verfassungsrechtlichen Gebots zur Gleichbehandlung wesentlich gleicher Sachverhalte nicht rechtfertigen. Mehr als zwei Jahre nach Aussprache der Empfehlung einer Gesetzesänderung durch den Petitionsausschuss ist noch immer keine Neuregelung erfolgt. Die verfassungswidrige Rechtslage bleibt sehenden Auges aufrechterhalten.

14.3 Sanktionslücke bei Verarbeitung von löschpflichtigen allgemein zugänglichen Daten

Die zentrale Bußgeldvorschrift des Bundesdatenschutzgesetzes zur Ahndung materiell unzulässiger Datenerhebungen und Datenverarbeitungen setzt als Tatobjekt personenbezogene Daten voraus, die nicht allgemein zugänglich sind. Im Einzelfall kann die Ausgrenzung allgemein zugänglicher Daten aus dem Kreis tauglicher Tatobjekte jedoch zu einer unbefriedigenden Sanktionslücke führen, wie der nachfolgende Fall zeigt:

Nach den Regelungen der Insolvenzordnung 1999 erfolgten öffentliche Bekanntmachungen der Insolvenzgerichte durch Veröffentlichung in dem für ihre amtlichen Bekanntmachungen jeweils bestimmten Blatt, also beispielsweise im Bundesanzeiger oder in regionalen Tageszeitungen. Ein Gläubiger eines Einzelgewerbetreibenden hatte seinerzeit beim zuständigen Gericht einen Insolvenzeröffnungsantrag bezüglich dessen Vermögen gestellt. Das Gericht hatte daraufhin zur vorläufigen Sicherung der Vermögensmasse des Schuldners Verfügungsbeschränkungen und die Bestellung eines vorläufigen Insolvenzverwalters beschlossen. Dieser Gerichtsbeschluss war entsprechend der Vorgabe der Insolvenzordnung öffentlich bekanntgemacht worden. Entsprechend der branchenüblichen Praxis zur Auswertung der öffentlichen Insolvenzgerichtsbekanntmachungen hatte eine Wirtschaftsauskunftei diesen Beschluss in ihren Datenbestand zu dem Einzelgewerbetreibenden übernommen. Nachdem das Gericht später den Insolvenzeröffnungsantrag des Gläubigers im Einzelnen geprüft und als unzulässig abgewiesen hatte, hatte es die Aufhebung der angeordneten Insolvenzsicherungsmaßnahmen beschlossen. Auch dieser Aufhebungsbeschluss war seitens des Gerichts öffentlich bekanntgemacht worden. Aus welchen Gründen auch immer hatte die Wirtschaftsauskunftei allerdings diesen Aufhebungsbeschluss nicht zur Kenntnis genommen und daher die im Datenbestand zu dem Einzelgewerbetreibenden gespeicherten Angaben zu den vorläufigen Insolvenzsicherungsmaßnahmen des Gerichts nicht gelöscht. Über etliche Jahre blieben daher unzutreffend Insolvenzangaben über den Einzelgewerbetreibenden gespeichert. Hinweise auf Insolvenz können quasi als „wirtschaftliches Todesurteil“ für eine Betroffene beziehungsweise für einen Betroffenen wirken. Erst nachdem diese unzutreffenden Angaben an Dritte, die eine Bonitätsauskunft einholten, übermittelt worden waren, wurde dem Einzelgewerbetreibenden die Speicherung bekannt.

Die Wirtschaftsauskunftei hatte also unter Verstoß gegen Löschpflichten Daten über etliche Jahre weitergespeichert und zu allem Überfluss auch noch an Dritte beauskunftet.

Da der seinerzeitige Gerichtsbeschluss zur Anordnung der vorläufigen Insolvenzsicherungsmaßnahmen veröffentlicht worden war, handelte es sich hierbei um allgemein zugängliche Daten. Auch durch den zwischenzeitlichen Zeitablauf hatte sich hieran nichts geändert. Denn letztlich war beziehungsweise ist die damalige papierne Veröffentlichung der angeordneten vorläufigen Insolvenzsicherungsmaßnahmen ohne rechtliche Zugangsschranken für jedermann recherchierbar. Damit lag zwar objektiv eine unbefugte Speicherung und Übermittlung personenbezogener Daten im Sinne der Bußgeldvorschrift vor. Tatobjekt waren jedoch allgemein zugängliche Daten, sodass eine Bußgeldahndung ausschied. Den Betroffenen blieben nur zivilrechtliche Ansprüche.

14.4 Bußgeldverfahren gegen Wirtschaftsauskunftei wegen wahrheitswidriger Eigenauskunft

Ein Bürger hatte unter Nutzung des im Webseiten-Servicebereich einer Wirtschaftsauskunftei vorgehaltenen Onlineformulars sein datenschutzrechtliches Auskunftsrecht geltend ge-

macht. Wenig später erhielt er an die angegebene E-Mail-Adresse eine offenkundig automatisiert generierte Antwort-E-Mail des Unternehmens. Hierin wurde ihm in einem lediglich durch die Anrede individualisierten Standardtext im Wesentlichen mitgeteilt, dass innerhalb der letzten zwölf Monate vor Zugang des Eigenauskunftsersuchens keine Daten zu seiner Person abgefragt worden sowie keine zu beauskunftenden Bonitätsdaten zu seiner Person vorhanden seien. Der Betroffene war allerdings in der Lage nachzuweisen, dass die Wirtschaftsauskunftei tags zuvor sehr wohl einem anderen Unternehmen online eine Wirtschaftsauskunft zu seiner Person erteilt hatte. Diese Auskunft hatte insbesondere auch negative Bonitätsdaten sowie Personenidentitätsdaten enthalten. Aufgrund dieser Wirtschaftsauskunft scheiterte ein beabsichtigter Vertragsschluss des Betroffenen.

Nachdem sich der Betroffene an uns gewandt hatte, leiteten wir wegen Erteilung einer unrichtigen wie unvollständigen Eigenauskunft nach § 34 Bundesdatenschutzgesetz ein selbstständiges Bußgeldverfahren gegen den Wirtschaftsauskunfteidienst ein. Im Rahmen der Anhörung erklärte dieser die Ursache der nicht ordnungsgemäßen Datenauskunft im Wesentlichen damit, dass der Betroffene zwei weitere Vornamen im Onlineformular angegeben hätte, die im System nicht hinterlegt gewesen seien. Man habe diesen Fall zum Anlass genommen, unmittelbar auf eine manuelle Beauskunftung umzustellen.

Damit war die Fehlbeauskunftung jedoch weder gerechtfertigt noch entschuldigt. Nach § 9 Satz 1 Bundesdatenschutzgesetz haben nicht öffentliche Stellen, die selbst personenbezogene Daten verarbeiten, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des Bundesdatenschutzgesetzes zu gewährleisten. Systeme, die eine vollautomatisierte Erteilung einer Eigenauskunft ermöglichen sollen, sind erkennbar von vornherein in höchstem Maße fehleranfällig. So ist bereits eine hinreichende Identifikation einer Auskunft erbittenden Person und Zuordnung zum vorhandenen Datenbestand nicht zuverlässig vollautomatisiert durchzuführen. In der Fehlbeauskunftung gegenüber dem anfragenden Betroffenen hatte sich dann prompt dieses Risiko verwirklicht. Auch die Umstellung auf manuelle Beauskunftung konnte die erteilte Fehlauskunft nicht aus der Welt schaffen, stellte nur den gebotenen rechtskonformen Zustand her.

Wir erließen deshalb einen Bußgeldbescheid, gegen den die Auskunftei Einspruch einlegte. Eine Begründung hierfür führte sie nicht an. Im Verhandlungstermin vor dem Amtsgericht machte sie lediglich geltend, dass die Geldbuße zu hoch bemessen sei. Zuvor hatte sie weder im Rahmen unserer Anhörung noch im Rahmen des bei uns eingelegten Einspruchs Angaben zu ihren wirtschaftlichen Verhältnissen gemacht. Daher waren wir bei der Zumessung der Geldbuße allein auf Schätzungen angewiesen gewesen. Die von uns festgesetzte Geldbuße wurde vom Amtsgericht reduziert.

Im Rahmen des parallel geführten Verwaltungsprüfverfahrens wollten wir uns vergewissern, ob die Wirtschaftsauskunftei nicht auch gegenüber anderen Auskunftssuchenden derart fehlerhafte Eigenauskünfte erteilt hatte. Wie es der Zufall wollte, hatte die Wirtschaftsauskunftei aber die Anfrageunterlagen und Auskunftsunterlagen des fraglichen Zeitraums gerade vernichtet.

Nicht zuletzt aufgrund der geschilderten Vorfälle bleibt die Wirtschaftsauskunftei im Fokus unserer Aufsichtstätigkeit.

15. Kreditwirtschaft und Versicherungen

15.1 N(ear)F(ield)C(ommunication) – Technik bei Zahlungskarten

Seit einiger Zeit gibt es verstärkt auch im Bereich des bargeldlosen Zahlungsverkehrs Bestrebungen, Zahlungskarten wie zum Beispiel die Bankkarten beziehungsweise Debitkarten, Kreditkarten et cetera mit der sogenannten N(ear)F(ield)C(ommunication) – Technik auszustatten. Hierbei handelt es sich um eine Nahbereichsfunktechnik, die es ermöglicht,

Informationen über einen Bereich von regelmäßig nur wenigen Zentimetern von der Zahlungskarte beziehungsweise ihrem Speicherchip zu einem Lesegerät zu übertragen. Eröffnet wird damit der Weg zu einem „kontaktlosen“ Leseverfahren; das Einführen der Zahlungskarte in ein Lesegerät ist nicht mehr nötig. Es genügt vielmehr, dass die Zahlungskarte für einen kurzen Moment in die Nähe eines Lesegeräts gehalten wird. Unter Umständen muss die Zahlungskarte nicht einmal mehr aus der Geldbörse entnommen werden. Die Zahlungsabwicklung soll hiermit noch bequemer und zügiger gestaltet werden. Die Ausstattung einer Zahlungskarte mit der NFC-Technik wird durch ein aufgebrachtes Piktogramm, das Funkwellen symbolisiert, angezeigt.

Sollen im Wege des Funkkontaktes auch personenbezogene beziehungsweise personenbeziehbare Informationen an ein Lesegerät übertragen werden, sind insoweit die Vorgaben des Datenschutzrechts zu beachten. Wer also Zahlungskarten mit dieser Technik ausgibt, hat datenschutzrechtlich neben der Gewährleistung einer sicheren Speicherung der personenbezogenen Daten insbesondere dafür Sorge zu tragen, dass nur eine gewollte Funkkommunikation stattfindet und die Daten während der Funkübertragung nicht durch unbefugte Dritte mitgelesen, verändert oder abgefangen werden können. Wenngleich die Zugriffsmöglichkeit unbefugter Dritte auf die Funkkommunikation durch die kurze Sendereichweite der Technologie eingeschränkt ist, bedarf es daher also auch spezifischer technischer und organisatorischer Sicherheitsvorkehrungen der Kartenherausgeber vor unbefugten Zugriffen auf den Funkdatenfluss. In Betracht kommen zum Beispiel Maßnahmen wie Verschlüsselung der übertragenen Daten, Initiierung einer Funkkommunikation nur bei Kontakt mit einem zugelassenen Lesegerät et cetera. Abhängig von Art und Umfang der gespeicherten und zu übertragenden Daten und der Missbrauchsgefahr steigen die Anforderungen an die Sicherheitsmaßnahmen. Daneben fordert das Bundesdatenschutzgesetz von den kartenausgebenden Stellen ein hohes Maß an Transparenz über die Technik. Sie müssen bei Ausgabe an den Kunden insbesondere in allgemein verständlicher Form über die Funktionsweise der Zahlungskarte mit NFC-Technik und die Art der verarbeiteten personenbezogenen Daten, über das „Wie“ der Ausübung datenschutzrechtlicher Betroffenenrechte sowie über erforderliche Maßnahmen bei Verlust oder Zerstörung der Zahlungskarte mit NFC-Technik unterrichten. Eine weitere zentrale Rechtsvorgabe ist es, dass das Ablaufen eines Funkkommunikationsvorgangs für den Betroffenen in irgendeiner Form eindeutig erkennbar gemacht werden muss.

Letztlich wird nur ein transparenter Umgang mit Chancen und Vorteilen aber auch Risiken der Technik, ein hohes technisches Sicherheitsniveau sowie schließlich die Einräumung einer Möglichkeit zur selbstbestimmten Entscheidung über die Nutzung der Technik bei Zahlungskarten zu einer breiten und langfristigen Akzeptanz bei den Kundinnen und Kunden führen. Denn es gibt Zahlungsvarianten, die aus datenschutzrechtlicher Sicht bereits im Ansatz weniger risikoträchtig sind und deren Nutzung keine wesentlichen Nachteile gegenüber dem kontaktlosen Zahlungsverfahren aufweist.

15.2 Datenübermittlung an das Hinweis- und Informationssystem der Versicherungswirtschaft

Ein Fahrzeughalter war mit seinem Auto in einen unverschuldeten Unfall verwickelt, was ihm durch die polizeiliche Aufnahme und Bearbeitung durch seine Kfz-Versicherung bestätigt worden war. Gleichwohl teilte die Versicherung ihrem Kunden mit, sie habe Daten seines Fahrzeuges (Kennzeichen und/oder Fahrzeugidentifizierungsnummer) an das Hinweis- und Informationssystem der Versicherungswirtschaft (HIS) gemeldet. Dieses System diene den beteiligten Versicherungsunternehmen zur Unterstützung der Sachverhaltsaufklärung bei Versicherungsfällen unter Rückgriff auf frühere Schadensfälle sowie zur Bekämpfung von Versicherungsmissbrauch. Die Daten würden zu einem späteren Zeitpunkt von dem jeweiligen Versicherer abgefragt und genutzt, wenn das Fahrzeug an einem weiteren Schadenfall beteiligt sein sollte. Es würden keine Daten zu seiner Person gespeichert.

Diese Auffassung der Kfz-Versicherung, bei dem beschriebenen Vorgehen würden keine Daten zur Person des Fahrzeughalters gespeichert, halten wir für falsch. Zumindest mit dem Kennzeichen des Kraftfahrzeugs kann ein aus HIS abrufendes Versicherungsunternehmen einen Bezug zur Person der Fahrzeughalterin oder des Fahrzeughalters herstellen, indem das Kennzeichen mit Auskünften aus dem Fahrzeugregister nach dem Straßenverkehrsgesetz kombiniert wird. Des Weiteren hatten wir Zweifel an der Zulässigkeit der Einmeldung und deren Speicherung.

Die Kfz-Versicherung teilte uns mit, eine Einmeldung der Fahrzeugdaten ins HIS sei vorgenommen worden, weil zunächst eine fiktive Abrechnung des Fahrzeugschadens erfolgt sei. Nach Einreichung der Reparaturrechnung sei die Abrechnungsart von fiktiv auf korrekt geändert worden, sodass nachträglich der Meldegrund entfallen sei. In der mit den Aufsichtsbehörden abgestimmten Arbeitsanweisung zu HIS sei festgelegt, dass der Meldegrund entfallen ist, wenn eine fiktive in eine konkrete Abrechnung geändert wird. Daher sei nach Angaben der Versicherung die Löschung der Daten inzwischen erfolgt. Im Übrigen teilte die Versicherung uns mit, dass es sich bei den ins HIS eingemeldeten Daten nunmehr auch aus ihrer Sicht um personenbezogene Daten des Fahrzeughalters handele.

16. Weitere Wirtschaftsunternehmen

16.1 Fehlende Einwilligung beim Namenswettbewerb für ein Eisbärenbaby

Eine Tagesausgabe einer Lokalzeitung enthielt einen Teilnahmecoupon für einen Namenswettbewerb für ein im Zoo am Meer in Bremerhaven geborenes Eisbärenbaby. Darin wurden Angaben zur Person, Anschrift und Telefonnummer erfragt. Gleichzeitig sollte eine Erklärung abgegeben werden, die es der Zeitung und den durch sie beauftragten Dienstleistern gestatten sollte, bei den am Wettbewerb Teilnehmenden telefonisch Angebote zu ihren Produkten zu machen. Da es sich um die Verarbeitung und Nutzung der Daten der Teilnehmerinnen und Teilnehmern zu Zwecken der Werbung handelte, waren die entsprechenden Bestimmungen des Bundesdatenschutzgesetzes und des Gesetzes gegen den unlauteren Wettbewerb anwendbar. Danach ist die Datenverarbeitung und Datennutzung für Werbezwecke nur mit ausdrücklicher Einwilligung der Betroffenen zulässig. Diese Anforderung lag hier nicht vor, sodass keine wirksamen Einwilligungen für Werbezwecke vorlagen, soweit Betroffene die Coupons ausfüllten und absendeten.

Auf unsere Anfrage reagierte die Zeitung unverzüglich und erklärte, die im Teilnahmecoupon angegebenen personenbezogenen Daten ausschließlich für die Verlosung nach Durchführung des Namenswettbewerbs für das Eisbärenbaby zu verwenden und danach zu löschen.

16.2 Fehlender Hinweis auf Widerspruchsrecht im Fitnessstudio

Eine gesetzliche Krankenkasse veranstaltete gemeinsam mit einem Fitnessstudio besondere Events. Dazu schrieb das Fitnessstudio seine Mitglieder an. Nach Angaben des Fitnessstudios erhielt die Krankenkasse keine Daten, sondern stellte lediglich Logopapier, Flyer und Briefumschläge für die Aktion zur Verfügung. In den Mitgliedschaftsverträgen wurde auf die Nutzung der Adressdaten für Werbung oder Marktforschung und Meinungsforschung hingewiesen. Hierzu enthält der Vertrag eine besondere Einwilligungserklärung. Da der Vertrag aber nicht den nach dem Bundesdatenschutzgesetz vorgeschriebenen Hinweis auf das Widerspruchsrecht der Betroffenen enthält, verlangten wir, diesen Hinweis ausdrücklich vorzunehmen. Seitdem weist das Fitnessstudio an seinem sogenannten Schwarzen Brett im Fitnessraum mit großer Schrift auf das Widerspruchsrecht hin.

16.3 Unerwünschte Newsletter

Ein Vermittler von Kulturveranstaltungen hatte das Verlangen eines Betroffenen, ihm keine weiteren Newsletter zuzusenden, trotz mehrfacher Erinnerungen ignoriert. Nachdem wir

eingeschaltet worden waren, verwies der Vermittler auf das Versehen eines Mitarbeiters. Zudem erklärte er, alle mit der Bearbeitung von Anliegen von Kundinnen und Kunden betrauten Beschäftigten seien auf die bevorzugte Bearbeitung von Auskunftsverlangen und Löschungsverlangen verpflichtet worden. Insbesondere sollten sie E-Mails von Kundinnen und Kunden täglich nach definierten Begriffen, beispielsweise „Datenschutz", „Daten löschen" oder „Account löschen" durchsuchen, um eine vorrangige Bearbeitung dieser Anliegen zu gewährleisten. Dies halten wir aus Sicht des Datenschutzes für ausreichend.

16.4 Nutzung des offenen Adressfeldes beim E-Mail-Versand

Immer wieder gehen bei den Datenschutzaufsichtsbehörden Beschwerden ein, weil Private wie auch Unternehmen beim Versand insbesondere von Newslettern das E-Mail-Adressfeld „An…" beziehungsweise „CC…" nutzen. Ein E-Mail-Versand über diese beiden Adressfelder hat im Unterschied zur Nutzung des Adressfelds „BCC…" zur Folge, dass der Empfängerin beziehungsweise dem Empfänger über die eigentliche Nachricht hinaus zugleich auch sämtliche E-Mail-Adressen der weiteren Mitempfängerinnen und Mitempfänger der Nachricht angezeigt werden. Mitunter nutzen dann sogar Mitempfängerinnen beziehungsweise Mitempfänger die neu erhaltenen E-Mail-Adressen für ihre eigenen Zwecke, zum Beispiel für den Versand eines eigenen Newsletters über die gleiche Verteilerliste. Da E-Mail-Adressen nach wie vor häufig aus Name, Vorname und nicht selten noch einem Zusatz, aus dem der Arbeitgeber hervorgeht, gebildet werden, handelt es sich in diesen Fällen regelmäßig um personenbezogene Angaben im Sinne des Datenschutzrechts.

In einem uns zur Kenntnis gelangten Fall hatte ein Unternehmensgeschäftsführer eine E-Mail zwecks Einladung zu einer Unternehmensveranstaltung an mehrere hundert Empfängerinnen und Empfänger über das Adressfeld „An…" versandt. Ausgedruckt wies allein die Adresszeile dieser E-Mail einen Umfang von etwa zehn DIN-A4-Seiten auf. Bei den E-Mail-Adressen handelte es sich zum Großteil um personenbezogene Angaben. Jedem Einzelnen der mehreren hundert Empfängerinnen und Empfängern wurden damit die E-Mail-Adressen der Mitempfängerinnen und Mitempfänger der E-Mail zugesandt. Selbstverständlich lagen weder Einwilligungen in die hundertfache Weitergabe der E-Mail-Adressen vor noch gab es eine gesetzliche Befugnisnorm, die diese Übermittlung gerechtfertigt hätte.

Da auch personifizierte E-Mail-Adressen keine belanglosen Angaben sind, das Ausmaß dieser getätigten rechtswidrigen Datenübermittlung so erheblich war und zudem bei dem Geschäftsführer aufgrund des Unternehmenstätigkeitsfeldes eine Sensibilität für Fragen des ordnungsgemäßen Datenumgangs hätte erwartet werden müssen, sahen wir uns zur Verhängung einer Geldbuße wegen Verstoßes gegen eine Bußgeldvorschrift des Bundesdatenschutzgesetzes veranlasst. Der Betroffene hatte die Fehlerhaftigkeit seines E-Mail-Versandes allerdings bereits unmittelbar nach Versand der E-Mail erkannt und sich sofort bei den Empfängerinnen und Empfängern der E-Mail entschuldigt. Dies berücksichtigten wir bei der Festlegung der Höhe der Geldbuße.

16.5 Missachtung des Auskunftsrechts

Beschwerden darüber, dass Daten verarbeitende Stellen das gesetzliche Recht auf Auskunft zu den zur Person gespeicherten personenbezogenen Angaben missachtet hätten, zählen zu den alltäglichen Eingaben bei uns und beschäftigten uns auch in diesem Berichtsjahr wieder mehrfach.

Lediglich ein Beschwerdefall sei aufgrund seiner Beispielhaftigkeit insoweit geschildert:

Eine Bürgerin hatte sich mittels Fax an ein größeres Dienstleistungsunternehmen gewandt und um Auskunft zu den dort zu ihrer Person gespeicherten Daten gebeten. Trotz Erinnerung mittels einer weiteren Faxanfrage blieb ihr Auskunftsersuchen unbeantwortet. Wir gingen auf das Unternehmen zu und baten um Erklärung. Das Unternehmen teilte uns

daraufhin mit, dass die Betroffene für ihr Auskunftsersuchen eine Telefaxnummer gewählt habe, die unternehmensintern dem für die Firmenkundenbetreuung zuständigen Mitarbeiterteam zugeordnet sei. Dort sei es leider versäumt worden, das Auskunftsersuchen an die zuständige Stelle im Unternehmen zur Bearbeitung weiterzuleiten.

Im Wege klarer interner organisatorischer Regelungen muss eine Daten verarbeitende Stelle sicherstellen, dass eingehende Eigenauskunftsgesuche an die intern für die Bearbeitung zuständige Stelle weitergeleitet und binnen angemessener Frist bearbeitet werden. Gleichwohl kann es selbstverständlich auch bei bester Organisation im Einzelfall einmal zu einem fehlerhaften Umgang mit einem Betroffenen-Auskunftsersuchen kommen. Im obigen Beschwerdefall waren allerdings die unternehmensinternen Vorgaben verbesserungsbedürftig. Da das Unternehmen jedoch umgehend reagierte, indem es die geforderte Auskunftserteilung gegenüber der Auskunftsbittenden nachholte und eine entsprechende Arbeitsanweisung gegenüber den Mitarbeiterinnen und Mitarbeitern anpasste, sahen wir keine Notwendigkeit für eine über die formlose Beanstandung hinausgehende aufsichtsbehördliche Reaktion.

16.6 Entsorgung von personenbezogenen Daten im Altpapiercontainer

Bei einer Freizeiteinrichtung entsprach es den Gepflogenheiten, nicht mehr benötigte Anmeldeformulare sowie liegengebliebene Rechnungsbelege der Besucherinnen und Besucher und sonstige Unterlagen in einem allgemein zugänglichen Altpapiercontainer zu entsorgen. Die Unterlagen waren dabei weder geschreddert noch waren die personenbezogenen Informationen sonst unleserlich gemacht.

Personen beziehungsweise Stellen, die automatisiert oder dateimäßig personenbezogene Daten verarbeiten, haben nach dem Bundesdatenschutzgesetz unter anderem stets sicherzustellen, dass kein Zugriff unbefugter Dritter auf diese personenbezogenen Informationen erfolgt. Die Anforderungen an die Sicherstellung dieses Ziels steigen insbesondere mit der Sensibilität der gespeicherten oder sonst verarbeiteten Informationen. Dies gilt selbstredend auch bei einer Entsorgung von Unterlagen mit personenbezogenen Informationen. Wer sich trotz eigener Verantwortlichkeit nicht um eine datenschutzrechtskonforme Entsorgung personenbezogener Informationen kümmert, muss unter Umständen mit einer Beseitigungsanordnung und gegebenenfalls auch der Verhängung einer Geldbuße rechnen.

Nachdem wir die Freizeiteinrichtung mit der Rechtslage konfrontiert hatten, zeigte sich diese nach kurzzeitigem anfänglichem Unverständnis einsichtig und sicherte die Beauftragung eines professionellen Entsorgungsfachbetriebs zu. Da wir erfreulicherweise keine weitergehenden Schadensfälle aus der nicht fachgerechten Entsorgung feststellen konnten und die Freizeiteinrichtung sich letztlich kooperativ zeigte, bestand keine Notwendigkeit weiterer aufsichtsbehördlicher Maßnahmen.

16.7 Ordnungswidrigkeitsverfahren wegen Nichtberücksichtigung von Werbewidersprüchen

Erneut erhielten wir eine Eingabe, bei der sich ein Bürger beklagte, von einem Unternehmen wiederholt Werbung erhalten zu haben, obwohl er der Nutzung seiner Daten für Zwecke der Werbung widersprochen habe. Er habe das Unternehmen aufgefordert, die Übersendung von Werbezuschriften an ihn zu unterlassen sowie seine Daten nicht weiter an Dritte zu übermitteln und diese sofort zu löschen. Außerdem habe er das Unternehmen gebeten, ihm seinen Widerspruch zu bestätigen und ihn aus dem Adressverteiler zu löschen.

Widersprechen von Datenverarbeitung Betroffene bei der verantwortlichen Stelle der Nutzung ihrer Daten für Zwecke der Werbung, ist eine Nutzung für diese Zwecke unzulässig. Unzulässig gespeicherte Daten sind zu löschen. Ordnungswidrig handelt, wer trotz des Widerspruchs der betroffenen Person Daten für Werbezwecke verarbeitet oder nutzt.

Trotz des Widerspruchs erhielt der Bürger von dem Unternehmen weitere Werbezuschriften. Im Rahmen der Anhörung teilte uns das Unternehmen mit, es habe den Widerspruch des Bürgers nicht erhalten. Diese Mitteilung war nicht glaubhaft, da sie durch eine entsprechende Bestätigung der Deutschen Post AG widerlegt wurde. Erst als wir tätig wurden, kam das Unternehmen seinen gesetzlichen Verpflichtungen nach. Daher gingen wir von einer vorsätzlichen Tatbegehung aus und verhängten ein Bußgeld in Höhe von 700 Euro.

17. Internationales und Europa

17.1 „Safe Harbor“ – Grundsätze zur Übermittlung von Daten in die USA

Im letzten Jahresbericht (vergleiche die Ziffern 1.1.2 und 18.2) stellten wir die Zulässigkeit von Datenübermittlungen in die Vereinigten Staaten von Amerika (USA) auf der Basis der Safe-Harbor-Entscheidung der Kommission der Europäischen Union (EU-Kommission) in Frage. Grund dafür sind die Enthüllungen von Edward Snowden über die anlasslose und flächendeckende Überwachung durch den US-amerikanischen Geheimdienst National Security Agency (NSA). Die EU-Kommission hat die Möglichkeit, die Safe-Harbor-Entscheidung jederzeit anzupassen, auszusetzen oder den Anwendungsbereich zu beschränken. Andererseits können die europäischen Aufsichtsbehörden für den Datenschutz nach der Safe-Harbor-Entscheidung Datentransfers in die USA aussetzen, wenn eine hohe Wahrscheinlichkeit besteht, dass die in der Entscheidung formulierten Grundsätze nicht eingehalten werden.

Ende November 2013 erklärte die EU-Kommission in einer Mitteilung an das Europäische Parlament und den Rat unter anderem, dass die Entscheidung überprüft werden müsse. Die bekannt gewordenen Informationen zu den Überwachungsprogrammen werfen neue Fragen über das Schutzniveau für personenbezogene Daten auf, das mit der Safe-Harbor-Entscheidung gewährleistet werden soll. Die groß angelegten Programme könnten dazu führen, dass die aufgrund des Safe-Harbor-Regelung transferierten Daten von US-Behörden über das Maß hinaus, das für den Schutz der nationalen Sicherheit unbedingt nötig und angemessen wäre, abgerufen und weiterverarbeitet würden. Ernsthaft in Frage stellte die EU-Kommission auch, ob Datenschutzrechte europäischer Bürgerinnen und Bürger, deren Daten in die USA übermittelt werden, angesichts des umfassenden Zugriffs der Nachrichtendienste auf Daten, die von Safe-Harbor-Unternehmen in die USA übermittelt werden, kontinuierlich geschützt seien. Auf dieser Grundlage empfahl die EU-Kommission bezüglich der Überwachungsmaßnahmen der US-Nachrichtendienste unter anderem, dass die entsprechenden Unternehmen in den USA Auskunft darüber geben sollten, in welchem Umfang US-Behörden nach Maßgabe des US-Rechts Daten erheben und verarbeiten dürften, die auf der Grundlage des der Safe-Harbor-Entscheidung übermittelt worden seien. Die Unternehmen sollten insbesondere angehalten werden, in ihren Datenschutzbestimmungen anzugeben, in welchen Fällen sie Safe-Harbor-Grundsätzen nicht beachteten, um Anforderungen der nationalen Sicherheit, des öffentlichen Interesses oder der Rechtsdurchsetzung der USA genügen zu können. Wichtig ist nach der Mitteilung der EU-Kommission, dass von der in der Safe-Harbor-Entscheidung vorgesehenen Ausnahme der nationalen Sicherheit nur so weit Gebrauch gemacht wird, wie dies unbedingt notwendig oder angemessen ist. Trotz dieser Bedenken erwog die bis Ende Oktober 2014 amtierende EU-Kommission keine Aussetzung des Safe-Harbor-Abkommens mit den USA. Wie sich die neue EU-Kommission verhalten wird, bleibt abzuwarten.

Ende Februar 2014 stellte das Europäische Parlament auf der Grundlage des Berichts seines Ausschusses für bürgerliche Freiheiten, Justiz und Inneres fest, dass es der Kommission nicht gelungen sei, auf die Beseitigung der hinreichend bekannten Mängel bei der derzeitigen Umsetzung der Safe-Harbor-Grundsätze hinzuwirken. Das Europäische Parlament forderte die Kommission und die Datenschutzaufsichtsbehörden auf, Datenübermittlungen in die USA, die sich auf die Safe-Harbor-Entscheidung stützen, unverzüg-

lich auszusetzen. Das Parlament verlangte, dass solche Datenübermittlungen auf der Grundlage anderer Instrumente erfolgten, sofern diese die erforderlichen Sicherheitsbestimmungen und Garantiebestimmungen für den Schutz der Privatsphäre sowie die Grundrechte und Freiheiten von Personen enthielten. Zudem forderte das EU-Parlament die EU-Kommission auf, bis Ende 2014 eine umfassende Bewertung des Rechtsrahmens der USA vorzulegen. Sie bestärkte die EU-Kommission darin, sich mit der US-Regierung auseinanderzusetzen, um einen Rechtsrahmen für ein hohes Datenschutzniveau zu schaffen und für die Gleichwertigkeit der in der Europäischen Union und in den Vereinigten Staaten von Amerika bestehenden Rahmenbedingungen für den Schutz der Privatsphäre zu sorgen. Aus den Verhandlungen der EU-Kommission mit den USA ist bisher nur bekannt geworden, bezüglich der Safe-Harbor-Entscheidung bestehe weiterhin ein Dissens.

Die Artikel-29-Datenschutzgruppe, ein Zusammenschluss der Aufsichtsbehörden der Mitgliedstaaten der Europäischen Union, stellte zudem im April 2014 fest, dass unter anderem die Safe-Harbor-Grundsätze nicht als Rechtsgrundlage herangezogen werden könnten, um die Übermittlung personenbezogener Daten an eine Drittstaatsbehörde zum Zwecke massiver und willkürlicher Überwachung zu rechtfertigen.

Die Aufsichtsbehörden für den Datenschutz innerhalb der Europäischen Union haben die Möglichkeit, gegenüber in ihrem jeweiligen Zuständigkeitsbereich ansässigen Unternehmen Datentransfers auf der Grundlage des Safe-Harbor-Abkommens auszusetzen. Gleichwohl ist hiervon noch nicht Gebrauch gemacht worden. Vorwiegend werden zunächst die Verhandlungen der EU-Kommission mit den USA abgewartet. Dies verzögert sich jedoch weiter angesichts des Amtsantritts der neuen EU-Kommission Anfang November letzten Jahres. Schließlich hat der irische High Court (Verfassungsgericht) den Europäischen Gerichtshof angerufen, um festzustellen, weshalb der irische Datenschutzbeauftragte in Bezug auf die US-Überwachungsprogramme nicht tätig geworden ist.

Ende des letzten Berichtsjahres schrieb der Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2014 den neugewählten Präsidenten der EU-Kommission, und bat ihn um Unterrichtung über den gegenwärtigen Verhandlungsstand zwischen der EU-Kommission und der US-Regierung über die Umsetzung der aufgezeigten Empfehlungen und um Mitteilung darüber, wann die EU-Kommission die Verhandlungen mit der US-Regierung zu beenden gedenke, und welche Maßnahmen sie ergreifen werde, wenn diese Verhandlungen nicht zu einem Ergebnis führten, das ein angemessenes Datenschutzniveau bei der Übermittlung von Daten von Bürgerinnen und Bürgern der EU in die USA sicherstelle.

Solange die USA nicht bereit sind, auf die anlasslose und flächendeckende Überwachung durch die NSA und damit den unzulässigen Zugriff auf personenbezogene Daten bei in den USA ansässigen Dienstleistern zu verzichten, sehen wir keine Möglichkeit, unter Berufung auf die Safe-Harbor-Entscheidung einen datenschutzkonformen Datentransfer in die USA zu gewährleisten. Wir raten Unternehmen im Land Bremen deshalb, auf die Übermittlung von Daten in die USA auf der Grundlage der Safe-Harbor-Entscheidung zu verzichten und stattdessen etwa Dienstleister mit Sitz innerhalb der Mitgliedstaaten der Europäischen Union und in Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum mit der Verarbeitung personenbezogener Daten zu beauftragen. Im November des Berichtsjahres versandten wir das erste offizielle Anhörungsschreiben im Anordnungsverfahren zur Aussetzung derartiger Datentransfers.

17.2 Datenschutz-Grundverordnung

In unserem 35. Jahresbericht (siehe Ziffer 1.2) berichteten wir ausführlich über den von der Kommission der Europäischen Union (EU-Kommission) Ende Januar 2012 vorgelegten Entwurf einer Datenschutz-Grundverordnung. Ende 2013 wurden die Beratungen des Europäischen Parlaments mit dem Bericht des Ausschusses für bürgerliche Freiheiten,

Justiz und Inneres zum Abschluss gebracht. Das Europäische Parlament hat eine Vielzahl von Änderungen vorgeschlagen, die die Rechte der Betroffenen stärken würden.

Beispielsweise wird der Begriff der personenbezogenen Daten – im Gegensatz zum Entwurf der EU-Kommission und entsprechend dem deutschen Datenschutzrecht – unter anderem auf bestimmte und bestimmbare Angaben festgelegt. Des Weiteren soll es nach den Vorschlägen des Parlamentes keine grundrechtsfreien Räume geben, weil keine Datenkategorien und Unternehmensgruppen (beispielsweise Kleinstunternehmen) aus dem Anwendungsbereich herausgenommen werden. Die Anforderungen an die Wirksamkeit von Einwilligungen und die Transparenz der damit verbundenen beabsichtigten Datenverarbeitung für die Betroffenen soll danach deutlich festgelegt werden. Außerdem schlägt das EU-Parlament vor, den Katalog der besonderen (sensiblen) Datenkategorien um Daten über verwaltungsrechtliche Sanktionen, Urteile und mutmaßliche Straftaten zu erweitern.

Bedeutsam ist auch der Änderungsvorschlag des EU-Parlaments zur Zuständigkeit der Aufsichtsbehörden für verantwortliche Stellen, die in mehreren Mitgliedstaaten personenbezogene Daten verarbeiten. Danach darf die federführende Aufsichtsbehörde, in deren Mitgliedstaat sich die Niederlassung einer verantwortlichen Stelle befindet, Maßnahmen erst nach Konsultation aller anderen zuständigen Aufsichtsbehörden ergreifen, muss sich dabei um einen Konsens bemühen und die Stellungnahmen der beteiligten Aufsichtsbehörden weitestmöglich beachten. Mit einer solchen Regelung würde es für Datenverarbeitern erschwert, sich die zuständige Aufsichtsbehörde durch Verlegung der Niederlassung selbst auszusuchen (siehe hierzu die Entschließung zur Struktur der künftigen Datenschutzaufsicht in Europa unter Ziffer 19.3 dieses Berichts).

Entgegen dem Entwurf der EU-Kommission, sich selbst das Letztentscheidungsrecht bei bestimmten Datenverarbeitungen vorzubehalten, schlägt das EU-Parlament vor, dieses Recht dem neuen unabhängigen Europäischen Datenschutzausschuss zu übertragen. Dies würde die Unabhängigkeit der Aufsichtsbehörden stärken. Darüber hinaus soll eine Vielzahl von Rechtsakten zu bestimmten Datenverarbeitungen auf der Grundlage der Grundverordnung vom unabhängigen Datenschutzausschuss und nicht von der EU-Kommission unter Einbeziehung der Aufsichtsbehörden festgelegt werden. Zudem sollen die Aufsichtsbehörden nach den Vorschlägen des EU-Parlaments Bußgelder bis zu einer Höhe von 100 Millionen Euro verhängen können, sodass derartige Androhungen spürbar und nicht zahnlos sein dürften.

Bedauerlicherweise haben weder das EU-Parlament noch die EU-Kommission eine Regelung vorgeschlagen, die es Mitgliedsländern erlaubt, für die Datenverarbeitung durch Stellen der öffentlichen Verwaltung Regelungen zu treffen, die im Hinblick auf die Sensitivität der Daten oder sonstiger Umstände über das Datenschutzniveau der Datenschutz-Grundverordnung hinausgehen. Für eine solche Regelung scheint sich die Bundesregierung jetzt in den Verhandlungen des Rates der Europäischen Union einzusetzen.

Der Rat der Europäischen Union (Zusammenschluss der Regierungen der EU-Mitgliedstaaten) hat bis Redaktionsschluss immer noch nicht abschließend über die Datenschutz-Grundverordnung beraten. Der für das Inkrafttreten der Grundverordnung erforderliche Trilog (Verhandlungen zwischen der EU-Kommission, dem Rat der Europäischen Union und dem Europäischen Parlament) kann daher nicht vor 2015 stattfinden.

18. Ordnungswidrigkeiten/Zwangsmittelverfahren

18.1 Ordnungswidrigkeitsverfahren

Auch im Berichtsjahr wurden von uns wieder Ordnungswidrigkeitsverfahren wegen unterschiedlicher Verstöße gegen das Bundesdatenschutzgesetz betrieben. Die Verfahren betrafen unter anderem die unbefugte Übermittlung von Rezeptdaten durch ein Rechenzentrum (siehe hierzu auch Ziffer 6.5 dieses Berichts), den unerwünschten Versand eines

Newsletters mit offener Adressverteilerliste (siehe hierzu auch Ziffer 16.4 dieses Berichts), die Nichtberücksichtigung von Werbewidersprüchen (Ziffer 16.7 dieses Berichts) und die Erteilung von Falschauskünften (Ziffer 18.2 dieses Berichts). Festgesetzt und eingezogen wurden Bußgelder in Höhe von bis zu 15.000 Euro.

In einigen Fällen wurde gegen unsere Bußgeldbescheide Einspruch eingelegt. Sofern wir den Einsprüchen nicht abhelfen konnten, leiteten wir die Vorgänge zur weiteren Bearbeitung an die Staatsanwaltschaft weiter. In diesen Fällen entscheiden dann letztlich die zuständigen Amtsgerichte über die Verhängung einer Geldbuße und deren Höhe. Auch können die Amtsgerichte das Ordnungswidrigkeitsverfahren einstellen.

18.2 Folgenlose Falschbeantwortung unseres Auskunftsgesuchs

Ein Handwerker befand sich in einer Auseinandersetzung mit einer Kundin zu der Frage, ob die vereinbarte Werkleistung ordnungsgemäß erbracht sei. Im Rahmen dieses Streits erhielt er eine E-Mail des Partners der Kundin, in der jener eine Einigung vorschlug. Um seinem Einigungsvorschlag Nachdruck zu verleihen und dem Handwerker die Aussichtslosigkeit weiterer Auseinandersetzung vor Augen zu führen, verwies der Partner der Kundin in seiner E-Mail auf seine Kenntnisse über die kritischen finanziellen Verhältnisse des Handwerkers und erläuterte dieses Wissen mit seiner Mitgliedschaft in einer Finanzauskunftei.

Der Handwerker wandte sich in Wahrnehmung seines Anrufungsrechts an uns und bat darum nachzuprüfen, ob es rechtens sei, dass Daten über seine finanziellen Verhältnisse durch einen Dritten, nicht am Werkvertrag Beteiligten, so ohne Weiteres abgerufen würden. Wie uns bekannt war, führte der Partner der Kundin als Einzelkaufmann einen Gewerbebetrieb. Es war daher nicht von vornherein auszuschließen, dass er wegen seiner Gewerbetätigkeit Mitglied einer Finanzauskunftei war und die allein zu geschäftlich bedingten Bonitätsprüfungen bestehende Abrufmöglichkeit in dem privaten Streitfall missbräuchlich genutzt hatte.

Wir wandten uns daher an den Partner der Kundin und forderten ihn unter Inanspruchnahme unseres gesetzlichen Auskunftsrechts und zugleich unter Belehrung über Voraussetzungen und Grenzen eines Auskunftsverweigerungsrecht auf, die folgende Frage zu beantworten: „Trifft es zu, dass Sie Mitglied bei der Auskunftei Z sind?“ Hierauf antwortete der Angeschriebene für sich in dritter Person: „Die Person Vorname X Name Y, wohnhaft (…) ist nicht Mitglied der Auskunftei Z.“ Um die Richtigkeit dieser Antwort zu überprüfen, befragten wir eine örtlich in Betracht kommende Auskunftei. Unser Auskunftsersuchen beantwortete sie dahingehend, dass „die Firma Vorname X Name Y, Gewerbebetrieb in (…)“ Mitglied sei.

Abweichend vom alltäglichen Sprachgebrauch ist eine „Firma“ nach den einschlägigen Regelungen des Handelsgesetzbuchs lediglich der Name eines Kaufmanns im Geschäftsverkehr. Eine Firma ist also nur ein Name, kein eigenes Rechtssubjekt. Da ein Einzelkaufmann eine natürliche Person und damit ein einziges Rechtssubjekt ist, handelt er unabhängig davon, ob es sich um den privaten oder den geschäftlichen Bereich handelt, als ein und dasselbe Rechtssubjekt, nur unter unterschiedlichen Namen. Als die Auskunftei uns mitteilte, Mitglied sei die Firma Vorname X Name Y, drückte sie damit also aus, dass das Mitglied der Partner der Kundin in eigener Person unter seinem Namen im Geschäftsverkehr sei. Seine Antwort an uns: „Die Person XY ist nicht Mitglied“, war daher erwiesenermaßen wahrheitswidrig.

Da wir nun wussten, dass der Partner der Kundin entgegen seiner Mitteilung doch eine Mitgliedschaft bei der Auskunftei innehatte und daher für ihn tatsächlich die Möglichkeit bestand, dass er seinen berufsmäßigen Zugang zu Bonitätsauskünften auch privat genutzt hatte, wandten wir uns neuerlich an ihn und setzten das Prüfverfahren unter Hinweis auf die bei Bonitätsabrufen zu wahrenden Gesetzesvorgaben fort. Der Betreffende teilte uns

mit, angesichts der umzusetzenden Gesetzesvorgaben auf seinen Onlinezugang und auf künftige Bonitätsabfragen verzichten zu wollen.

Da nach dem Bundesdatenschutzgesetz die Erteilung einer unrichtigen Auskunft auf ein Ersuchen der Datenschutzaufsichtsbehörde hin eine Ordnungswidrigkeit darstellt, leiteten wir zugleich ein Bußgeldverfahren wegen vorsätzlicher Falschbeauskunftung ein. Nachdem wir einen Bußgeldbescheid erlassen hatten, legte der Betroffene Einspruch ein. Wir sahen keinen rechtlichen Grund, diesem Einspruch abzuhelfen und legten daher dem zuständigen Gericht, Strafabteilung, auf dem vorgeschriebenen Weg über die Staatsanwaltschaft den Bußgeldbescheid nebst Akte zur Entscheidung vor.

Zu unserer Überraschung vertrat auch das Gericht zunächst die Auffassung, die Person Vorname X Name Y sei nicht Mitglied der Auskunftei. Die uns erteilte Auskunft sei daher wahr gewesen, das Bußgeldverfahren könne eingestellt werden.

Wir wiesen auf die Regelung des Handelsgesetzbuchs hin. Gleichwohl stellte das Gericht letztlich das Bußgeldverfahren ein. Die vom Gericht zur Verfahrenseinstellung genutzte Vorschrift des Ordnungswidrigkeitengesetzes setzt voraus, dass eine Ordnungswidrigkeit festgestellt wurde, aber nach nicht begründungspflichtiger subjektiver Einschätzung des Gerichts kein Ahndungsbedürfnis besteht. Das Gericht ging also von einer Falschauskunft aus, verneinte aber aus uns nicht bekannten Gründen das Ahndungsbedürfnis und legte der Staatskasse die Kosten des Verfahrens auf.

18.3 Zwangsmittelverfahren

Im Berichtsjahr betrieben wir in mehreren Fällen Zwangsmittelverfahren. Die hiervon betroffenen Unternehmen waren trotz unserer wiederholten Aufforderungen ihren datenschutzrechtlichen Verpflichtungen nicht nachgekommen. Hierbei ging es insbesondere um die Erteilung von Auskünften an uns als Aufsichtsbehörde, zu denen die für die Datenverarbeitung verantwortlichen Stellen gesetzlich verpflichtet sind. Auch die Erfüllung der Pflicht zur Meldung von Verfahren automatisierter Verarbeitungen sowie die Pflicht zur Löschung von Kundendaten waren Gegenstand der Zwangsmittelverfahren.

Angedroht und festgesetzt wurden Zwangsgelder in Höhe von bis zu 2.000 Euro. Wir leiteten in den Fällen Mahnverfahren und Vollstreckungsverfahren ein, in denen rechtskräftig festgesetzte Zwangsgelder nicht bezahlt wurden.

19. Die Entschließungen der Datenschutzkonferenzen im Jahr 2014

19.1 Beschäftigtendatenschutzgesetz jetzt!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. März 2014)

Trotz zahlreicher Aufforderungen durch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie des Deutschen Bundestages ist die Verabschiedung einer angemessenen Regelung des Beschäftigtendatenschutzes in der vergangenen Legislaturperiode erneut gescheitert. Der Koalitionsvertrag für die 18. Legislaturperiode sieht vor, das nationale Datenschutzniveau im Beschäftigtendatenschutz bei den Verhandlungen zur europäischen Datenschutz-Grundverordnung zu erhalten und darüber hinausgehende Standards zu ermöglichen. Falls mit einem Abschluss der Verhandlungen über die europäische Datenschutz-Grundverordnung nicht in angemessener Zeit gerechnet werden kann, soll eine nationale Regelung geschaffen werden.

Dies reicht nicht aus. Wann die Datenschutz-Grundverordnung verabschiedet wird, ist derzeit völlig unklar. Ohnehin ist mit einem Inkrafttreten dieser europäischen Regelungen schon aufgrund der notwendigen Umsetzungsfrist erst in einigen Jahren zu rechnen. Aufgrund

der voranschreitenden technischen Entwicklung, die eine immer weitergehende Mitarbeiterüberwachung ermöglicht, besteht unmittelbarer Handlungsbedarf. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung deshalb auf, ein nationales Beschäftigtendatenschutzgesetz umgehend auf den Weg zu bringen. Die Formulierung „in angemessener Zeit“ lässt befürchten, dass der Beschäftigtendatenschutz in dieser Legislaturperiode schon wieder auf die lange Bank geschoben wird.

Ein Beschäftigtendatenschutzgesetz muss ein hohes Datenschutzniveau gewährleisten und einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem Recht auf informationelle Selbstbestimmung des Arbeitnehmers schaffen.

Dies wird erkennbar in den vielfältigen Fragestellungen, für die es bislang keine klaren rechtlichen Vorgaben gibt. Zu nennen sind hier beispielsweise die immer umfassendere Videoüberwachung, Dokumentenmanagementsysteme, die die Leistung der Beschäftigten transparent werden lassen, die zunehmende Verquickung von Arbeit und Privatem verbunden mit der dienstlichen Nutzung von privaten Arbeitsmitteln wie Handy und Laptop, die Nutzung von dienstlich zur Verfügung gestellten Kraftfahrzeug mit oder ohne die Erlaubnis privater Nutzung oder die private Nutzung der vom Arbeitgeber zur Verfügung gestellten E-Mail-Zugänge und Internetzugänge, der zunehmende Einsatz biometrischer Verfahren sowie die Erhebung und Verarbeitung von Bewerberdaten beispielsweise aus sozialen Netzwerken.

Hierfür müssen künftig gesetzliche Standards geschaffen werden, um sowohl die Rechtssicherheit für die Arbeitgeber zu erhöhen als auch einen wirksamen Grundrechtsschutz für die Beschäftigten zu schaffen.

19.2 „Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!“

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. März 2014)

Die Nutzung biometrischer Daten wird zunehmend zu einem Phänomen des Alltags. Dies gilt in besonderer Weise für die biometrische Gesichtserkennung, die in sozialen Medien auf dem Vormarsch ist. Für den Zweck der Auswertung von Personenfotos werden die Gesichter der Nutzer biometrisch erfasst, sodass ein späterer Abgleich mit anderen Fotos die Identifizierung einzelner Personen ermöglicht. Dazu werden sogenannte Templates erstellt. Dies sind mathematische Modelle der wesentlichen Merkmale des Gesichts wie etwa dem Abstand von Augen, Mundwinkel und Nasenspitze. Es darf nicht verkannt werden, dass die Vermessung der Gesichtsphysiognomie in hohem Maße die schutzwürdigen Interessen Betroffener berührt, denn stets ist die dauerhafte Speicherung eines Referenz-Templates des eigenen Gesichts erforderlich.

Dass die Templates dann in den Datenbanken global agierender Internetunternehmen gespeichert werden, stellt nicht erst seit den Enthüllungen über das Überwachungsprogramm Prism, das den US-Geheimdiensten den Zugriff auf die Datenbanken der US-Anbieter erlaubt, ein erhebliches Risiko für das Persönlichkeitsrecht des Einzelnen dar.

Die biometrische Gesichtserkennung ist eine Technik, die sich zur Ausübung von sozialer Kontrolle eignet und der damit ein hohes Missbrauchspotenzial immanent ist. Mit ihrer Hilfe ist es möglich, aus der Flut digitaler Fotografien im Internet gezielt Aufnahmen von Zielpersonen herauszufiltern. Darüber hinaus könnten durch den Abgleich von Videoaufnahmen mit vorhandenen Templates in Echtzeit Teilnehmerinnen und Teilnehmer etwa von Massenveranstaltungen sowie von Demonstrationen oder einfach nur Passanten individualisiert und identifiziert werden. Der Schutz der Anonymität des Einzelnen in der Öffentlichkeit lässt sich damit zerstören, ohne dass die Betroffenen ihre biometrische Überwachung kontrollieren oder sich dieser entziehen können.

An die Erzeugung biometrischer Templates der Gesichter von Personen durch Internetdienste sind daher hohe rechtliche Anforderungen zu stellen, die das informationelle Selbstbestimmungsrecht von Betroffenen in höchstmöglicher Weise berücksichtigen:

— Die Erhebung, Verarbeitung und/oder Nutzung biometrischer Daten zur Gesichtserkennung zum Zweck der Erstellung eines dauerhaften biometrischen Templates kann nur bei Vorliegen einer wirksamen Einwilligung des Betroffenen im Sinne des § 4a Bundesdatenschutzgesetz (BDSG) rechtmäßig erfolgen.

— Die Einwilligung in die Erstellung biometrischer Templates zur Gesichtserkennung muss aktiv und ausdrücklich durch den Betroffenen erteilt werden. Die Betroffenen müssen vor der Erteilung der Einwilligung über die Funktionsweise der Erstellung und Nutzung der sie möglicherweise betreffenden Templates und die damit verfolgten Zwecke und Risiken in klarer und verständlicher Weise umfassend informiert werden. Eine Zweckänderung ist unzulässig. Sie bedarf einer Einwilligung, die dem Standard an die Einwilligungen bei der Verarbeitung besonderer personenbezogener Daten, § 4a Absatz 3 BDSG, entspricht.

— Die Einwilligung kann nicht durch den Verweis auf entsprechende Klauseln in allgemeinen Nutzungsbedingungen oder Datenschutzerklärungen ersetzt werden.

— Für eine logische Sekunde kann es nach § 28 Absatz 1 Satz 1 Nummer 2 beziehungsweise Nummer 3 BDSG auch ohne Einwilligung zulässig sein, ein Template zu erstellen, mit dem ein Abgleich mit bereits vorhandenen, zulässigerweise gespeicherten Templates im Rahmen des von der Einwilligung abgedeckten Zwecks möglich ist. Betroffene sind über den Umstand, dass Bilder zum Abgleich mit bestehenden Templates verwendet werden, zu informieren.

— Derartige biometrische Templates zum automatischen Abgleich, bei denen eine Einwilligung fehlt, sind unverzüglich nach dem Abgleich zu löschen.

— Die Speicherung von biometrischen Templates von Dritten, die – anders als die Nutzer von sozialen Medien – regelmäßig nicht einwilligen können, ist ausgeschlossen.

19.3 Entschließung zur Struktur der künftigen Datenschutzaufsicht in Europa

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. März 2014)

Ein zentrales Verhandlungsthema bei den Beratungen im Rat der Europäischen Union (EU) betrifft die Frage, welche Aufgaben die Datenschutzbehörden künftig haben und wie sie in Fällen, die mehrere Mitgliedstaaten oder die gesamte EU betreffen, besser zusammenarbeiten können. Die Europäische Kommission hatte hierzu das Prinzip einer einheitlichen Anlaufstelle („One-Stop-Shop“) vorgeschlagen, wonach die Datenschutzbehörde am Sitz der Hauptniederlassung EU-weit zuständig ist für die Aufsicht über alle Niederlassungen eines Unternehmens innerhalb der EU. Daneben schlug sie die Einführung eines Kohärenzverfahrens vor, das es den Datenschutzbehörden ermöglichen soll, in grenzüberschreitenden Fällen zu einheitlichen Entscheidungen im Rahmen des europäischen Datenschutzausschusses zu gelangen.

Vor dem Hintergrund der aktuell im Rat erörterten unterschiedlichen Modelle plädieren die Datenschutzbeauftragten des Bundes und der Länder für einen effektiven und bürgernahen Kooperationsmechanismus und Entscheidungsmechanismus, der folgende Kernelemente beinhalten sollte:

1. Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen den Grundsatz, dass jede Aufsichtsbehörde im Hoheitsgebiet ihres Mitgliedstaats die ihr mit der Verordnung übertragenen Aufgaben und Befugnisse über alle Datenverarbeitungen aus-

übt, durch welche Personen dieses Mitgliedstaates betroffen sind, unabhängig davon, ob die verantwortliche Stelle über eine Niederlassung innerhalb dieses Mitgliedstaates verfügt oder nicht.

2. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die Einführung eines One-Stop-Shop-Mechanismus für Fälle, in denen der Datenverarbeiter über mehrere Niederlassungen in unterschiedlichen EU-Mitgliedstaaten verfügt. In diesem Fall fungiert die Aufsichtsbehörde am Ort der Hauptniederlassung als federführende Behörde, die mit den Aufsichtsbehörden der Mitgliedstaaten, in denen der Verantwortliche über weitere Niederlassungen verfügt oder in denen Personen betroffen sind, eng kooperiert. Es bleibt damit den betroffenen Personen unbenommen, sich an die Aufsichtsbehörden ihres Heimatlandes zu wenden.

3. Die federführende Behörde und die mit zuständigen nationalen Aufsichtsbehörden kooperieren mit dem Ziel einer einheitlichen Entscheidungsfindung. Im Falle der Einigkeit erlässt die federführende Behörde die erforderlichen Maßnahmen gegenüber der Hauptniederlassung des Verantwortlichen. Der Verantwortliche ist verpflichtet, die Maßnahmen in allen Niederlassungen innerhalb der EU umzusetzen.

4. Sofern eine nationale Behörde dem Maßnahmenentwurf der federführenden Behörde widerspricht, ist der Europäische Datenschutzausschuss mit dem Fall zu befassen, der hierzu verbindliche Leitlinien erlassen oder sonstige verbindliche Maßnahmen treffen kann.

5. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die in dem Verordnungsentwurf enthaltenen Elemente zur Stärkung der Verantwortlichkeit der Unternehmen zur Einhaltung des Datenschutzrechts. Hierzu zählen die EU-weite Einführung betrieblicher Datenschutzbeauftragter, Datenschutz-Folgeabschätzungen, Privacy-by-Design und Privacy-by-Default, Zertifizierungen, Datenschutzsiegel und Verhaltensregeln. Fragen zur Rechtskonformität einer Datenverarbeitung können im Rahmen der vorherigen Zurateziehung mit den Aufsichtsbehörden geklärt werden.

6. Für die Einführung formeller, fristgebundener Verfahren zur Erlangung EU-weit gültiger Compliance-Entscheidungen besteht aus Sicht der Datenschutzbeauftragten des Bundes und der Länder daneben kein Bedarf. Insbesondere darf die Klärung von Compliance-Fragen nicht zu einer Verlagerung der Verantwortlichkeit auf die Aufsichtsbehörden und zur Einschränkung aufsichtsbehördlicher Maßnahmen im Falle von Datenschutzverstößen führen.

7. Ein originärer Schwerpunkt der Aufsichtstätigkeit in Bezug auf Zertifizierungsprozesse sollte darin liegen, im Rahmen der Norminterpretation Prüfstandards mitzugestalten, auf deren Grundlage die Vergabe von Zertifikaten geprüft wird.

19.4 „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. März 2014)

Die Enthüllungen des Whistleblowers Edward Snowden haben ein Ausmaß an geheimdienstlicher Überwachung aufgezeigt, das viele zuvor nicht für möglich gehalten hatten. Die tendenziell unbegrenzte und kaum kontrollierte Überwachung der elektronischen Kommunikation aller verletzt das auch im digitalen Zeitalter weltweit anerkannte Recht auf Privatheit in täglich wiederkehrender millionenfacher Weise. Dies beeinträchtigt zugleich die Wahrnehmung anderer Menschenrechte wie der Meinungs- und Versammlungsfreiheit. Es ist eine gesamtgesellschaftliche Aufgabe, berechtigtes Vertrauen in die prinzipielle Unverletzlichkeit der Kommunikation wiederherzustellen.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher schon im September 2013 gefordert, auf diese neue Qualität der Überwachung rechtlich und politisch

zu reagieren. Darüber hinaus sind aber auch technische und organisatorische Schutzmaßnahmen erforderlich. Der Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen sowie der Vertraulichkeit und Integrität informationstechnischer Systeme muss wiederhergestellt und dauerhaft gesichert werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Prüfung und Umsetzung folgender Maßnahmen:

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten,
2. Bereitstellung einer einfach bedienbaren Verschlüsselungs-Infrastruktur,
3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verfahren zur Verbindungsverschlüsselung,
4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten,
5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten,
6. Ausbau der Angebote und Förderung anonymer Kommunikation,
7. Angebot für eine Kommunikation über kontrollierte Routen,
8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung,
9. Beschränkung des Cloud Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit,
10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung,
11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik,
12. Ausreichende Finanzierung von Maßnahmen der Informationssicherheit.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz hat einen Anforderungskatalog formuliert, der die hier genannten Maßnahmen konkretisiert (siehe Anlage zu dieser Entschließung).

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter elektronischer Kommunikationsdienste auf, entsprechende Technologien und Dienste zur Verfügung zu stellen. Die Verwaltungen in Bund und Ländern, insbesondere die zuständigen Regulierungsbehörden, sind aufgefordert, auf die Durchsetzung der oben genannten Maßnahmen zu dringen. Der Gesetzgeber ist aufgerufen, die zu ihrer Durchsetzung gegebenenfalls nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen.

Anlage
zur Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. März 2014 in Hamburg

„Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten als wesentliches Element für den Schutz von Daten

Der verschlüsselte Transport und die verschlüsselte Speicherung von Daten müssen zu einem in Produkte und Verfahren integrierten Standard werden, der durch jedermann einfach zu nutzen ist. Sichere kryptografische Algorithmen, die seit vielen Jahren zur Ver-

fügung stehen, stellen auch für Geheimdienste eine erhebliche Hürde dar und erschweren die unberechtigte Kenntnisnahme der so geschützten Daten wesentlich. Für die Sicherung der Übertragungswege sollen Verfahren zum Einsatz kommen, die eine nachträgliche Entschlüsselung des abgeschöpften Datenverkehrs erschweren (perfect forward secrecy).

2. Bereitstellung einer von jeder Person einfach bedienbaren Verschlüsselungs-Infrastruktur

Für eine breite Anwendung von Verschlüsselung durch die Bürgerinnen und Bürger wird eine Infrastruktur benötigt, die es jeder Person weitgehend ohne Barrieren (in Form von Wissen, nötiger spezieller Software oder finanziellen Mitteln) ermöglicht, den von ihr verwendeten Kommunikationsadressen Schlüssel authentisch zuzuordnen und die anderer zu nutzen. Die Entstehung dieser Infrastruktur bedarf der Förderung durch den Staat unter Einbeziehung bestehender Instrumente beispielsweise durch Entwicklung kryptografischer Zusatzfunktionen des neuen Personalausweises.

Es mangelt also nicht vorrangig an theoretischen Konzepten, sondern an einer ausreichenden Durchdringung in der Praxis. Der öffentliche wie der private Sektor müssen daher ihre Anstrengungen erhöhen, Verschlüsselungstechniken selbst einzusetzen und in ihre Produkte und Dienstleistungen einzubinden.

3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verbindungsverschlüsselung

Der Einsatz von Mechanismen für eine Ende-zu-Ende-Verschlüsselung muss gefördert werden. Die Enthüllungen von Edward Snowden haben gezeigt, dass der Zugriff auf Daten besonders einfach ist, wenn sie an Netzknoten unverschlüsselt vorliegen oder innerhalb interner Netze unverschlüsselt übertragen werden. Nur eine Ende-zu-Ende-Verschlüsselung ist in der Lage, die Inhaltsdaten auch an diesen Stellen zu schützen. Die zusätzliche Verschlüsselung der Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) hingegen schützt die Metadaten der Kommunikation in allen Zwischenknoten der verschlüsselten Wegstrecke. Durch die Kombination beider Verfahren kann ein Optimum an Schutz zwischen den Endpunkten erreicht werden.

Für beide Ansätze stehen etablierte Verfahren zur Verfügung, sowohl in Bezug auf kryptografische Verfahren und Datenformate, als auch in Bezug auf das Identitätsmanagement und Schlüsselmanagement, von dessen Stringenz die Sicherheit wesentlich abhängt.

4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten

Sämtliche Internetangebote öffentlicher Stellen sollten standardmäßig über TLS (Transport Layer Security) / SSL (Secure Socket Layer) unter Beachtung der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik angeboten werden. Die Behörden sollten sich hierbei mit Zertifikaten ausweisen, die von vertrauenswürdigen Ausstellern herausgegeben wurden, die sich in europäischer und vorzugsweise in öffentlicher Hand befinden. Nicht öffentliche Stellen stehen gleichermaßen in der Verpflichtung, die Nutzung von ihnen angebotener Telemedien einschließlich der von einem Nutzer abgerufenen URIs (Uniform Resource Identifier) gegen Kenntnisnahme Dritter im Rahmen der Verhältnismäßigkeit durch Verschlüsselung zu schützen.

5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten

Die von der Wissenschaft bereits untersuchten Methoden metadatenarmer E-Mail-Kommunikation müssen weiterentwickelt und sowohl für E-Mail als auch für andere nachrichtenbasierte Kommunikationsformate alltagstauglich gemacht werden. Denn auch eine wirksame Ende-zu-Ende-Verschlüsselung verhindert nicht, dass beim E-Mail-Versand Metada-

ten anfallen, die aussagekräftige Rückschlüsse auf die Kommunikationspartner und deren Standorte zulassen. Die an die Öffentlichkeit gelangten Dokumente von Geheimdiensten haben gezeigt, dass allein durch Analyse der E-Mail-Metadaten riesige Datenbanken gefüllt wurden, mit denen nachvollzogen werden kann, wer mit wem von welchem Ort aus kommuniziert hat.

6. Ausbau der Angebote und Förderung anonymer Kommunikation

Verfahren zur anonymen Nutzung von Internet und Telekommunikationsangeboten müssen gefördert und entsprechende Angebote ausgebaut werden. Nutzerinnen und Nutzer müssen Anonymisierungsdienste nutzen können, ohne dass ihnen daraus Nachteile entstehen. Die Einbindung derartiger Konzepte trägt substantiell zur Umsetzung der gesetzlich normierten Forderung nach Datensparsamkeit bei und verringert die Gefahr missbräuchlicher Nutzung von Daten.

7. Angebot für eine Kommunikation über kontrollierte Routen

Deutsche und internationale Provider sollen Angebote zur Verfügung stellen, über selbst bestimmte Wege untereinander zu kommunizieren. Möglichst kurze, geografisch lokale Routen können gegebenenfalls die Wahrscheinlichkeit illegitimen Eingriffs in den Datenstrom reduzieren. Kontrollmöglichkeiten über die Datenströme werden verbessert, wenn die Kommunikation vollständig über eigene Leitungen abgewickelt oder verschlüsselt wird.

Solche Konzepte dürfen jedoch nicht verwechselt werden mit der Kontrolle des Internet oder Versuchen, Teile davon abzuschotten – dies wäre in jeder Hinsicht kontraproduktiv. Sie müssen daher sowohl anbieterneutral als auch supranational angegangen werden und setzen optimal direkt bei den zugrunde liegenden technischen Standards an.

8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung

Die Kommunikation mittels mobiler Geräte und der Zugang zum Internet mit Hilfe mobiler Kommunikationstechnik müssen den gleichen Datenschutzanforderungen und Sicherheitsanforderungen wie denen bei drahtgebundener Kommunikation genügen. Dazu gehört sowohl eine wirksame Verschlüsselung als auch die Geheimhaltung von Daten, die zur Lokalisierung der Nutzerinnen und Nutzer genutzt werden können. Der Schutz des Fernmeldegeheimnisses durch die Mobilfunkanbieter wird dadurch gefördert, dass

— alle Übertragungswege – sowohl vom Gerät zur Basisstation, als auch innerhalb des Netzwerks des TK-Anbieters – verschlüsselt werden,

— für die Verschlüsselung vom Mobilgerät zur Basisstation im GSM-Netz mindestens die Chiffre A5/3 zur Anwendung kommt, bis eine nachhaltig sichere Nachfolgechiffre zur Verfügung steht,

— eine Authentifizierung der Basisstationen gegenüber den Mobilgeräten erfolgt (diese Funktionalität bedarf der Unterstützung durch die vom TK-Anbieter bereitgestellte SIM-Karte) und

— die Kenntnis von Lokalisierungsdaten auf die Betreiber der Netze, in welche das jeweilige Gerät sich einbucht, und den Betreiber seines Heimatnetzes beschränkt wird.

Die Bundesnetzagentur sollte im Rahmen ihrer Aufgaben und Befugnisse aktiv auf die TK-Anbieter zur Durchsetzung dieser Maßnahmen einwirken.

Ferner bedarf es einer internationalen Anstrengung zur Anpassung oder Neudefinition von Standards für Mobilfunknetzwerke aller Generationen mit dem Ziel, die durchgreifende

Gewährleistung von Vertraulichkeit der Inhaltsdaten sowie der Vertraulichkeit und Datensparsamkeit der Verkehrsdaten und Standortdaten zu ermöglichen.

Wie für TK-Anbieter, so gilt auch für Anbieter von Telemedien für die mobile Nutzung, insbesondere in Form mobiler Anwendungen (Apps), dass sie die Erhebung von personenbezogenen Daten auf das für die jeweils erbrachte Dienstleistung erforderliche Minimum beschränken müssen und die Übertragung dieser Daten durch Verschlüsselung schützen sollten. Apps sollten künftig so durch Nutzerinnen und Nutzer konfigurierbar sein, dass diese selbst bestimmen können, wem welche Daten zu welchem Zweck übermittelt werden.

9. Beschränkung des Cloud Computings mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheitstechnik

Sollen personenbezogene Daten in einer Cloud-Anwendung verarbeitet werden, so dürfen nur Anbieter zum Zuge kommen, deren Vertrauenswürdigkeit sowohl in Bezug auf die Gewährleistung der Informationssicherheit, als auch in Bezug auf den Rechtsrahmen, innerhalb dessen sie operieren, gegeben ist.

Dazu gehören unter anderem ein (zertifiziertes) Informationssicherheitsmanagement, die sichere Verschlüsselung der zu verarbeitenden Daten sowohl bei ihrer Übertragung in und aus der Cloud als auch bei ihrer Speicherung und eine durch den Auftraggeber kontrollierte Vergabe von Unteraufträgen. Das Datenschutzniveau dieser Dienste sollte durch unabhängige und fachkundige Auditoren geprüft und zertifiziert werden.

10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung

Hardware und Software sollten so entwickelt und hergestellt werden, dass Anwenderinnen und Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit der getroffenen Sicherheitsvorkehrungen überzeugen können. Open-Source-Produkte ermöglichen derartige Prüfungen besonders gut. Daher ist der Einsatz von Open-Source-Produkten zu fördern.

Darüber hinaus ist es erforderlich, die bereits bestehenden Zertifizierungsverfahren für informationstechnische Produkte und die Informationssicherheit von Verarbeitungsvorgängen breiter zur Anwendung zu bringen und um weitere Zertifizierungsverfahren zu ergänzen, um die Vertrauenswürdigkeit von informationstechnischen Produkten zu stärken. Voraussetzung dafür sind unabhängige und fachkundige Auditoren sowie transparente Kriterienkataloge und Zertifizierungsprozesse.

11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik

Viele technische Vorkehrungen zum Schutz elektronisch übermittelter und gespeicherter Daten entfalten nur dann ihre volle Wirksamkeit, wenn die Nutzerinnen und Nutzer deren Vorteile kennen, mit diesen Vorkehrungen umgehen können und sie selbst einsetzen. Daher ist eine breit angelegte Bildungsoffensive erforderlich, mit der die notwendigen Kenntnisse und Fähigkeiten vermittelt werden.

12. Ausreichende Finanzierung für Maßnahmen der Informationssicherheit

Die Ausgaben der öffentlichen Hand für Informationssicherheit müssen erhöht werden und in einem angemessenen Verhältnis zum gesamten IT-Budget stehen. Die Koalitionspartner auf Bundesebene haben die Bundesbehörden bereits verpflichtet, zehn Prozent des IT-Budgets für die Sicherheit zu verwenden. Dies muss in angemessener Weise auch für Landesbehörden und andere öffentliche Stellen gelten. Die Ressourcen werden sowohl für die Planung und Absicherung neuer Vorhaben, insbesondere des E Governments, als auch für die Revision und sicherheitstechnische Ergänzung der Verfahren und der Infrastruktur im Bestand benötigt.

19.5 „Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke – Strenge Regeln erforderlich!“

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. März 2014)

Mit zunehmender Beliebtheit sozialer Netzwerke bei Bürgerinnen und Bürgern steigt das Interesse von Strafverfolgungsbehörden, diese sozialen Netzwerke auch zur Öffentlichkeitsfahndung zu nutzen. So gibt es in Deutschland bereits Polizeidienststellen, die mittels Facebook nach Straftätern suchen. Auch die 84. Konferenz der Justizministerinnen und Justizminister hat sich im November 2013 mit dem Thema befasst.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es erneut für notwendig darauf hinzuweisen, dass eine Nutzung sozialer Netzwerke privater Betreiber (wie zum Beispiel Facebook) zur Öffentlichkeitsfahndung aus datenschutzrechtlicher Sicht sehr problematisch ist. Durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten wird in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener (Tatverdächtiger oder auch Zeugen) eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist. Auch sind im Internet veröffentlichte Daten einer Fahndungsausschreibung nur sehr schwer beziehungsweise gar nicht mehr zu löschen. Geben Nutzerinnen und Nutzer der sozialen Netzwerke in Diskussionsforen und Nutzerkommentaren öffentlich Spekulationen, Behauptungen und Diskriminierungen ab, beeinträchtigt dies die Persönlichkeitsrechte der Betroffenen erheblich. Solche Funktionen sind in von den Ermittlungsbehörden betriebenen Angeboten weder geeignet noch erforderlich, um die behördlichen Aufgaben zu erfüllen. Die Konferenz weist darauf hin, dass Öffentlichkeitsfahndung nur auf Diensten von Anbietern erfolgen darf, die die datenschutzrechtlichen Vorgaben des Telemediengesetzes zur Nutzungsdatenverarbeitung, insbesondere der Regeln zur Reichweitenmessung gemäß §§ 13 Absatz 4 Nummer 6, 15 Absatz 3 Telemediengesetz (TMG), und das Recht auf anonyme und pseudonyme Nutzung gemäß § 13 Absatz 6 TMG beachten.

Sofern es Strafverfolgungsbehörden gleichwohl gestattet werden soll, zu Zwecken der Öffentlichkeitsfahndung auf soziale Netzwerke mit deaktivierter Kommentierungsfunktion zurückzugreifen, so darf dies – ungeachtet der generellen Kritik an der Nutzung sozialer Netzwerke durch öffentliche Stellen – nur geschehen, wenn folgende Maßgaben beachtet werden:

— Die Vorschriften der Strafprozessordnung (§ 131 Absatz 3, § 131a Absatz 3, § 131b Strafprozessordnung [StPO]) zur Öffentlichkeitsfahndung kommen aufgrund der technikoffenen Formulierung als Rechtsgrundlage für die Öffentlichkeitsfahndung im Internet grundsätzlich in Betracht. Sie sind aber im Hinblick auf den Verhältnismäßigkeitsgrundsatz nur eingeschränkt anzuwenden. Eine entsprechende Klarstellung durch den Gesetzgeber wäre wünschenswert. Zumindest aber sind die besonderen Voraussetzungen der Fahndung im Internet, insbesondere in sozialen Netzwerken, in Umsetzungsvorschriften zu konkretisieren. Änderungsbedarf besteht beispielsweise für die Anlage B der RiStBV (Richtlinie für das Strafverfahren und das Bußgeldverfahren).

— In materiell-rechtlicher Hinsicht haben die Strafverfolgungsbehörden den Verhältnismäßigkeitsgrundsatz strikt zu beachten. Die zu schaffenden Regelungen müssen den besonderen Gefahren der Öffentlichkeitsfahndung in sozialen Netzwerken gerecht werden. Insbesondere muss sichergestellt werden, dass eine solche Fahndung nur bei im Einzelfall schwerwiegenden Straftaten überhaupt in Betracht gezogen werden kann.

— In verfahrensrechtlicher Hinsicht müssen die Umsetzungsregelungen die Staatsanwaltschaft verpflichten, bereits im Antrag auf richterliche Anordnung der Maßnahme die Art, den Umfang und die Dauer der Öffentlichkeitsfahndung konkret anzugeben.

Dies umfasst insbesondere die ausdrückliche Angabe, ob und warum die Anordnung auch die Öffentlichkeitsfahndung in sozialen Netzwerken umfassen soll.

— Es ist sicherzustellen, dass

  – die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert und verarbeitet werden, nicht hingegen auf Servern der privaten Anbieter,

  – die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Web-Crawler und ähnliche Dienste so weit als technisch möglich verhindert werden,

  – die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzern nur außerhalb der sozialen Netzwerke erfolgt.

19.6 Ende der Vorratsdatenspeicherung in Europa!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. April 2014)

Der Europäische Gerichtshof hat in seinem Urteil vom 8. April 2014 die Europäische Richtlinie zur Vorratsspeicherung von Telekommunikations-Verkehrsdaten (Richtlinie 2006/24/EG) für ungültig erklärt. Dieses Urteil hat weitreichende Folgen für den Datenschutz in Europa.

Die Datenschutzbeauftragten des Bundes und der Länder haben die anlasslose und massenhafte Speicherung von Verkehrsdaten der Telekommunikation stets abgelehnt. Sie begrüßen die Entscheidung des Europäischen Gerichtshofs als wichtigen Schritt zur Bekräftigung der informationellen Selbstbestimmung und des Telekommunikationsgeheimnisses.

Der Europäische Gerichtshof hat in seinem Urteil der undifferenzierten und automatischen Totalerfassung solcher Daten eine klare Absage erteilt. Er hat darauf hingewiesen, dass schon die Pflicht zur anlasslosen Speicherung einen besonders schwerwiegenden Eingriff großen Ausmaßes in das Recht auf Privatleben und den Datenschutz der Betroffenen darstellt. Diese in der Europäischen Grundrechte-Charta verbrieften Rechte dürften nur eingeschränkt werden, soweit dies absolut notwendig ist.

Die für ungültig erklärte Richtlinie entsprach diesen Vorgaben nicht, weil sie ohne jede Differenzierung, Einschränkung oder Ausnahme zur pauschalen Totalerfassung der Verkehrsdaten verpflichtete. Nach dem Urteil des Gerichtshofs kann eine undifferenzierte Pflicht zur anlasslosen und flächendeckenden Vorratsdatenspeicherung unionsrechtlich nicht mehr neu begründet werden. Die Absichtserklärung der Bundesregierung, zurzeit kein Gesetz zur Speicherung von Verkehrsdaten einzuführen, wird von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt. Etwaige Diskussionen auf europäischer Ebene sollten abgewartet werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist ausdrücklich darauf hin, dass der Maßstab des Europäischen Gerichtshofs auch für das anlasslose exzessive Überwachen durch sämtliche Nachrichtendienste gelten muss.

Zudem hält der Gerichtshof die Pflicht zur großflächigen Speicherung von personenbezogenen Daten nur dann für zulässig, wenn die Daten in der Europäischen Union gespeichert werden und damit unter die Kontrolle unabhängiger Datenschutzbehörden fallen. Dies zwingt auch zu einer Neubewertung zum Beispiel der Fluggastdaten-Übermittlung in die Vereinigten Staaten von Amerika und des Safe-Harbor-Abkommens.

19.7 Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014)

Der Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen. Die Datenverarbeitung in modernen Fahrzeugen schafft Begehrlichkeiten, die dort anfallenden Daten für die verschiedensten Zwecke nutzen zu wollen – etwa bei Arbeitgebern und Versicherungen. Dabei besteht die Gefährdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergeräten und nicht erst mit deren Auslesen oder Übermitteln. Bereits diese personenbezogenen Daten geben Auskunft über Fahrverhalten und Aufenthaltsorte und können zur Informationsgewinnung über den Fahrer beziehungsweise den Halter bis hin zur Bildung von Persönlichkeitsprofilen herangezogen werden.

Um eine selbstbestimmte Fahrzeugnutzung frei von Furcht vor Überwachung zu gewährleisten, sind Automobilhersteller, Händler, Verkäufer, Werkstätten ebenso wie Anbieter von Kommunikationsdiensten und Telediensten rund um das Kraftfahrzeug im Rahmen ihres Wirkungskreises in der Pflicht, informationelle Selbstbestimmung im und um das Kraftfahrzeug zu gewährleisten.

Dazu gehört:

— Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote für Kommunikationsdienste und Teledienste die Datenschutzgrundsätze von Privacy-by-Design beziehungsweise Privacy-by-Default zu verwirklichen.

— Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zugrunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.

— Die Datenverarbeitungen müssen entweder vertraglich vereinbart sein oder sich auf eine ausdrückliche Einwilligung stützen.

— Für Fahrer, Halter und Nutzer von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden. Änderungen sind rechtzeitig anzuzeigen. Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzer ebenfalls zu informieren.

— Auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübermittlung an den Hersteller oder sonstige Diensteanbieter sind Fahrer, Halter und Nutzer technisch und rechtlich in die Lage zu versetzen, Datenübermittlungen zu erkennen, zu kontrollieren und gegebenenfalls zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.

— Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und Datenintegrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.

Auf dieser Grundlage wirkt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder daraufhin, dass Automobilhersteller, Zulieferer und ihre Verbände bundesweit

einheitliche Datenschutzstandards auf hohem Niveau setzen, die dazu beitragen, dass Innovation auch mit gesellschaftlicher Akzeptanz einhergeht.

19.8 Unabhängige und effektive Datenschutzaufsicht für Grundrechtsschutz unabdingbar

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014)

Die Bundesregierung hat am 27. August 2014 einen Gesetzentwurf zur Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund beschlossen (siehe Bundesrat Drucksache 395/14). Er sieht vor, dass die bisher beim Bundesministerium des Inneren eingerichtete Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in eine eigenständige oberste Bundesbehörde umgewandelt wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass nunmehr auch der Bundesgesetzgeber die vom Europäischen Gerichtshof in mehreren Urteilen konkretisierten Voraussetzungen für eine völlig unabhängige Datenschutzaufsicht herstellen will. Es ist erfreulich, dass die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit künftig keiner Aufsicht durch eine andere Behörde mehr unterliegen wird und aufgrund ihres Status als eigenständiger oberster Bundesbehörde ohne jeden Einfluss anderer Behörden selbst über ihren eigenen Haushalt und ihr eigenes Personal verfügen kann.

Die Konferenz weist jedoch auf wesentliche Punkte hin, denen auch der Gesetzentwurf keine beziehungsweise nur unzureichend Rechnung trägt:

— Eine effektive Datenschutzaufsicht setzt die rechtliche Stärkung der Durchsetzungsbefugnisse der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zwingend voraus. Ihr müssen in ihrem Zuständigkeitsbereich gegenüber den Postanbietern und Telekommunikationsanbietern die gleichen Anordnungsbefugnisse und Untersagungsbefugnisse eingeräumt werden, wie sie den Aufsichtsbehörden der Länder gegenüber der Privatwirtschaft schon seit Jahren zustehen. Der Bundesbeauftragten ist in diesem Bereich auch die Stellung einer Obersten Bundesbehörde und Bußgeldbehörde einzuräumen. Nur dann stehen auch ihr wirksame Eingriffsbefugnisse, wie sie die europäische Datenschutzrichtlinie fordert, zur Verfügung.

— Eine unabhängige, funktionsfähige und effektive Datenschutzkontrolle setzt zudem voraus, dass die BfDI als künftige oberste Bundesbehörde mit ausreichenden personellen und sächlichen Mitteln ausgestattet ist, um ihren gesetzlichen Kontrollaufgaben und Beratungsaufgaben nachkommen zu können. Entsprechendes gilt für alle Datenschutzbehörden in den Ländern. Ebenso wie in vielen Ländern ist dies für die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit im vorliegenden Entwurf des Bundesdatenschutzgesetz nicht der Fall.

— Die Genehmigung, als Zeugin auszusagen, wird durch den Gesetzentwurf in problematischer Weise eingeschränkt. Zwar wird der generelle Genehmigungsvorbehalt des Bundesministeriums des Innern aufgehoben, das Gesetz sieht aber weite Ausnahmen hiervon vor, diese sind zu streichen. Zumindest muss das Letztentscheidungsrecht bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verbleiben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, der Bundesbeauftragten sowohl effektive Sanktionsmöglichkeiten an die Hand zu geben als auch die nötigen Personalmittel für eine den Aufgaben entsprechende Personalausstattung zur Verfügung zu stellen. Die Konferenz erinnert auch die Länder daran, dass auch sie ihren Datenschutzaufsichtsbehörden ausreichend Personalmittel

zur Verfügung stellen müssen, um die bereits bestehenden Kontrolldefizite zulasten der Bürgerinnen und Bürger und deren Grundrechtsschutz abzubauen.

19.9 Effektive Kontrolle von Nachrichtendiensten herstellen!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014)

Die Enthüllungen über die Spähaktivitäten ausländischer Nachrichtendienste haben verdeutlicht, wie viele Kommunikationsdaten in der digitalisierten Welt anfallen, welche Begehrlichkeiten diese Daten offensichtlich auch bei Nachrichtendiensten demokratischer Länder wecken und mit welchen weitreichenden Methoden die Nachrichtendienste Informationen erfassen, sammeln und analysieren. Auch die deutschen Nachrichtendienste haben weitreichende Befugnisse zur Erhebung, Sammlung und Auswertung personenbezogener Daten sowie zum Austausch dieser untereinander beziehungsweise mit Polizeibehörden. Die Befugnisse der Nachrichtendienste schließen auch die Überwachung der Telekommunikation ein. Damit einher geht im Bereich der strategischen Auslandsüberwachung des Bundesnachrichtendienstes ein Kontrolldefizit. Auch eine Beteiligung des Bundesnachrichtendienstes durch Datenaustausch mit ausländischen Diensten steht im Raum. In den vergangenen Jahren wurden die gesetzlichen Befugnisse der Nachrichtendienste stetig erweitert. So wurden die Antiterrordatei und die Rechtsextremismusdatei als gemeinsame Dateien von Polizei und Nachrichtendiensten eingeführt sowie gemeinsame Zentren von Nachrichtendiensten und Polizeibehörden errichtet. Die Berichte der Untersuchungsausschüsse zur Terrorgruppe Nationalsozialistischer Untergrund (NSU) des Deutschen Bundestages und einiger Landesparlamente haben darüber hinaus erhebliche Kontrolldefizite auch bei den Verfassungsschutzämtern offengelegt. Nach der Einschätzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist daher eine Reform der rechtsstaatlichen Kontrolle der deutschen Nachrichtendienste dringend geboten.

Für die Betroffenen ist die aufgrund der Befugnisse der Nachrichtendienste und Sicherheitsbehörden vorgenommene Datenverarbeitung in weitem Maße intransparent, daher ist auch der Individualrechtsschutz faktisch eingeschränkt. Umso wichtiger ist die Kontrolle durch unabhängige Stellen. In der Entscheidung zum Antiterrordateigesetz vom 24. April 2013 hat das Bundesverfassungsgericht insoweit hervorgehoben, dass der Verhältnismäßigkeitsgrundsatz bei Datenverarbeitungen, die für die Betroffenen nur eingeschränkt transparent sind, gesteigerte Anforderungen an eine wirksame Ausgestaltung der Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis stellt. Eine wichtige Rolle kommt dabei den Datenschutzbeauftragten des Bundes und der Länder zu, die neben den parlamentarischen Kontrollinstanzen die Kontrolle über die Nachrichtendienste ausüben. Bestimmte Bereiche nachrichtendienstlicher Tätigkeiten sind der Eigeninitiativkontrolle durch die Datenschutzbeauftragten des Bundes und der Länder von vornherein entzogen. Es ist sinnvoll, das bei den Datenschutzbeauftragten des Bundes und der Länder bereits vorhandene Fachwissen auch in diesem Bereich zu nutzen und die Datenschutzbehörden mit den entsprechenden Prüfbefugnissen und den hierfür erforderlichen personellen Ausstattungen und Sachmitteln auszustatten.

Das Bundesverfassungsgericht hat mit der Entscheidung vom 24. April 2013 zum Zusammenwirken zwischen den Datenschutzbeauftragten und den parlamentarischen Kontrollinstanzen festgestellt: „Wenn der Gesetzgeber eine informationelle Kooperation der Sicherheitsbehörden vorsieht, muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen.“ In diesem Sinne darf die Verteilung der Kontrolle auf mehrere Stellen nicht die Effektivität der Kontrolle einschränken. Für den Bereich der Telekommunikationsüberwachung nach dem Gesetz zur Beschränkung des Briefgeheimnisses, Postgeheimnisses und Fernmeldegeheimnisses ist die Kontrolle durch die G10-Kommission aus eigener Initiative derzeit gesetzlich nicht vorgesehen. Ebenso fehlt ein Kontrollmandat der Datenschutzbeauftragten für Beschränkungen des Fernmeldegeheimnisses. Vor dem

Hintergrund der Ausführungen des Bundesverfassungsgerichtes erscheint eine Einbindung der Datenschutzbeauftragten neben den parlamentarischen Kontrollinstanzen aber erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Gesetzgeber auf, die Datenschutzbehörden mit entsprechenden Prüfbefugnissen auszustatten, damit das bei ihnen vorhandene Fachwissen auch in diesem Bereich genutzt werden kann.

19.10 Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014)

Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 13. Mai 2014 – C-131/12 „Google Spain“ einen fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet geleistet. Die Namenssuche in Suchmaschinen kann erhebliche Auswirkungen auf die Persönlichkeitsrechte haben. Mit Suchmaschinen lassen sich weltweit in Sekundenschnelle detaillierte Profile von Personen erstellen. Oft sind Einträge über eine unbegrenzte Zeit hinweg abrufbar. Sie können dann zu sozialen und wirtschaftlichen Nachteilen für die Betroffenen führen, die gegebenenfalls ein Leben lang mit früheren oder vermeintlichen Verfehlungen konfrontiert bleiben. Das Urteil stellt nun klar, dass die Betreiber von Suchmaschinen ein Recht Betroffener auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen umzusetzen haben. Künftig bleiben die Betroffenen daher nicht nur darauf angewiesen, ihre Ansprüche unmittelbar gegenüber den Informationsanbietern zu verfolgen, die häufig nur schwer oder auch gar nicht zu realisieren sind.

Betroffene können sich nun auch direkt an die Suchmaschinenbetreiber wenden und verlangen, dass bei der Suche einzelne Links zu ihrem Namen künftig nicht mehr angezeigt werden.

Das Urteil ordnet dabei allerdings nicht an, bestimmte Inhalte, wie Presseartikel oder Artikel aus der Wikipedia, zu löschen oder ihre Auffindbarkeit im Internet unmöglich zu machen. Vielmehr soll – nach einer erfolgreichen Beschwerde des Betroffenen – der entsprechende Link lediglich bei Eingabe eines bestimmten Personennamens nicht mehr angezeigt werden. Der betroffene Inhalt bleibt mit allen anderen Suchbegriffen weiterhin frei zugänglich (für Inhalte, die regelmäßig durch Eingabe des Namens einer Person in eine Suchmaschine gefunden werden, weil es sich um eine Person des öffentlichen Lebens handelt, hat der EuGH ausdrücklich eine Ausnahme vorgesehen).

Zu Recht wird in der Debatte auf die erhebliche Macht der Anbieter von Suchmaschinen hingewiesen, über die Veröffentlichung von Suchergebnissen zu entscheiden. Diese Macht besteht jedoch nicht erst seit der Entscheidung des EuGH. Tatsächlich haben Inhalteanbieter keinen Rechtsanspruch am Nachweis ihrer Inhalte durch Suchmaschinen. Anbieter von Suchmaschinen sind keine neutralen Sachwalter der Informationsgesellschaft, sondern kommerziell handelnde Wirtschaftsunternehmen. Welche Suchergebnisse den Nutzern angezeigt wurden, bestimmt sich damit jedenfalls auch nach den kommerziellen Interessen von Suchmaschinen und ihren Vertragspartnern. Darüber hinaus unterlagen Suchmaschinen auch bereits vor der Entscheidung des EuGH bei der Gestaltung der Suchergebnisse äußeren Beschränkungen (zum Beispiel durch das Urheberrecht). Mit dem Urteil wird klargestellt, dass Suchmaschinen neben diesen Erwägungen jetzt auch die Grundrechte der Betroffenen zu berücksichtigen haben.

Das Urteil konkretisiert die Kriterien, unter welchen sich ausländische Unternehmen an europäisches beziehungsweise nationales Datenschutzrecht halten müssen. Dieses für den Grundrechtsschutz maßgebliche Urteil muss nunmehr von den Suchmaschinenbetreibern umfassend umgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auf folgende Punkte hin:

— Die effektive Wahrung der Persönlichkeitsrechte des Betroffenen setzt voraus, dass Anbieter von Suchmaschinen die Suchergebnisse bei einem begründeten Widerspruch weltweit unterbinden. Angesichts der territorialen Unbeschränktheit des Internet muss der Schutz des Einzelnen vor einer unberechtigten Verbreitung personenbezogener Daten universell gelten.

— Der verantwortliche Betreiber der Suchmaschine hat regelmäßig die Rechte der Betroffenen gegen die Interessen der Öffentlichkeit an einem freien und umfassenden Informationszugang im Einzelfall abzuwägen. Dabei ist insbesondere auf die Schwere der Persönlichkeitsrechtsbeeinträchtigung, die Stellung des Betroffenen im öffentlichen Leben sowie auf den zeitlichen Ablauf zwischen der Veröffentlichung und dem Antrag des Betroffenen beim Suchmaschinenbetreiber abzustellen.

— Die Entscheidung über die Verbreitung von Suchergebnissen, die Umsetzung von Widersprüchen und die Abwägungsentscheidung mit dem öffentlichen Interesse treffen zunächst die Suchmaschinenbetreiber. Die Kontrolle dieser Entscheidungen obliegt den jeweiligen Aufsichtsbehörden für den Datenschutz oder den staatlichen Gerichten. Alternative Streitbeilegungsverfahren oder Streitschlichtungsverfahren dürfen das verfassungsmäßige Recht der Betroffenen auf eine unabhängige Kontrolle durch die dafür vorgesehenen staatlichen Institutionen nicht beschneiden.

— Eine Befugnis der Anbieter von Suchmaschinen, Inhaltsanbieter routinemäßig über die Sperrung von Suchergebnissen zu informieren, besteht nicht. Dies gilt auch dann, wenn die Benachrichtigung nicht ausdrücklich den Namen des Betroffenen enthält.

19.11 Marktmacht und informationelle Selbstbestimmung

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014)

Die Konzentration wirtschaftlicher Macht und der Missbrauch marktbeherrschender Stellungen ist bisher Gegenstand des Wettbewerbsrechts und insbesondere des Kartellrechts. So untersucht gegenwärtig die Europäische Kommission mögliche Verstöße von Google gegen das europäische Wettbewerbsrecht wegen mangelhafter Neutralität der Suchergebnisse.

Darüber hinaus ist jedoch zu lange übersehen worden, dass die zunehmenden Unternehmenskäufe vor allem im Bereich der Internetwirtschaft zu einer massiven Anhäufung von personenbezogenen Daten bis hin zur Monopolbildung in bestimmten Bereichen führen können. Datenmacht wird zur Marktmacht. Im April 2007 kaufte Google für 3,1 Milliarden US-Dollar das Werbeunternehmen Double-Click. Die Übernahme wurde sowohl von den Kartellbehörden in den Vereinigten Staaten von Amerika (USA) und in Europa gebilligt, ohne dass die Auswirkungen dieser Übernahme auf den Datenschutz der Nutzer in diesen Entscheidungen berücksichtigt worden wäre. Facebook hat im vergangenen Jahr für die Übernahme von WhatsApp 18 Milliarden US-Dollar gezahlt. Auch dieser Zusammenschluss ist inzwischen sowohl in den USA als auch in der EU genehmigt worden, ohne dass es wirksame Garantien gegen eine weitere Verschlechterung des Datenschutzes gibt.

Sowohl der Europäische Datenschutzbeauftragte als auch die deutsche Monopolkommission haben inzwischen auf die möglichen Auswirkungen der Zusammenschlüsse gerade von solchen Internetunternehmen auf die informationelle Selbstbestimmung hingewiesen, deren Geschäftsmodelle wesentlich auf der Anhäufung von personenbezogenen Daten beruhen. Die massive Ausweitung von scheinbar kostenlosen Diensten und die wachsende Bedeutung von „Big Data“ erfordert nach Ansicht des Europäischen Datenschutzbeauftragten einen intensiveren Dialog zwischen den Datenschutzbehörden und den Kartell-

behörden, um die Wahlfreiheit wie auch die informationelle Selbstbestimmung der Nutzer angesichts abnehmender Konkurrenz aufrechtzuerhalten oder wiederherzustellen und um die Aufsichtsbefugnisse koordiniert einzusetzen. Die Monopolkommission hat in ihrem XX. Hauptgutachten (2012/2013 – Kapitel I) für eine verstärkte Kooperation von Datenschutzbehörden und Wettbewerbsbehörden plädiert und sich für eine schnelle Verabschiedung der Europäischen Datenschutz-Grundverordnung eingesetzt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder setzt sich ebenfalls für eine Datenschutz-Grundverordnung auf hohem Niveau ein. Sie ist davon überzeugt, dass insbesondere das Recht auf Datenportabilität sowohl die Souveränität des einzelnen Nutzers stärken als auch die auf der Sammlung personenbezogener Daten beruhende Machtposition einzelner Marktteilnehmer begrenzen kann.

Die Konferenz der Datenschutzbeauftragten weist daraufhin, dass eine stärkere Zusammenarbeit mit den Kartellbehörden sinnvoll ist. Ziel muss es dabei zugleich sein, den Datenschutz im Wettbewerb besser zu fördern.

19.12 Keine Pkw-Maut auf Kosten des Datenschutzes!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. November 2014)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) fordert die Bundesregierung auf, bei der geplanten Einführung einer allgemeinen Maut auf Bundesautobahnen und einzelnen Bundesfernstraßen auf eine automatisierte Erhebung, Verarbeitung und Nutzung von Fahrzeugkennzeichen aller Verkehrsteilnehmer über elektronische Kontrollpunkte zu verzichten. Für Abrechnungszwecke und Kontrollzwecke besteht hierfür kein Erfordernis, denn es stehen – beispielsweise durch Einführung einer physischen Vignette nach dem Vorbild anderer Staaten – mildere und gleichermaßen effektive Mittel zur Kontrolle der Entrichtung der Maut zur Verfügung, ohne täglich an hunderten Kontrollpunkten hunderttausende Kfz-Kennzeichen zu erfassen und zu speichern. Für die Kontrolle in Deutschland zugelassener Pkw ist die (optisch-)elektronische Überwachung schon deswegen nicht erforderlich, weil die Abrechnung über die Zulassungs-Steuerdaten und Kfz-Steuerdaten erfolgen soll. Allein die Möglichkeit, sich die Infrastrukturabgabe für gänzlich ungenutzte Pkw erstatten zu lassen, rechtfertigt nicht die vorgesehene elektronische Erfassung und sogar dauerhafte – bis zu 13 Monaten währende – Speicherung von Bewegungsdaten in Deutschland zugelassener Pkw.

Die DSK lehnt die im Entwurf eines Infrastrukturabgabengesetzes geplante Einrichtung eines Zentralen Infrastrukturregisters beim Kraftfahrtbundesamt und einer Datei sämtlicher mautpflichtiger Autobahnnutzungen von Personenkraftwagen beim Bundesamt für Güterverkehr ab. Ebenso weist sie auf die Gefahren der Einbeziehung privater Betreiber in die Erhebung der Infrastrukturabgabe einerseits und eines privaten Dritten in die Überwachung der Infrastrukturabgabe andererseits im Hinblick auf die umfangreichen geplanten Befugnisse der Betreiber beziehungsweise des Dritten zur Datenerhebung und Datenverarbeitung hin. Die DSK mahnt die Bundesregierung eindringlich zur Einhaltung der verfassungsrechtlich gebotenen Prinzipien der Datenvermeidung und Datensparsamkeit.

19.13 Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. November 2014)

Zur Verbesserung der Versorgung von Krebspatienten bauen die Bundesländer derzeit auf bundesgesetzlicher Grundlage ein flächendeckendes Netz von klinischen Krebsregistern auf. Diese Register erhalten hierzu vielfältige Daten über alle krebskranken Per-

sonen von allen niedergelassenen Ärzten und Krankenhäusern, die sie behandeln. Andererseits sollen die Register den behandelnden Ärzten die empfangenen Patientendaten zum Abruf zur Verfügung stellen. Die hierbei übermittelten Daten sind hoch sensibel und können mannigfaltig missbraucht werden. Dem müssen die Maßnahmen zu ihrem Schutz entsprechen.

Mit dieser Entschließung legt die Konferenz einen Katalog von Anforderungen vor und ruft die Bundesländer auf, für deren Erfüllung bei der Ausgestaltung der Kommunikation zwischen medizinischen Leistungserbringern und den klinischen Krebsregistern Sorge zu tragen.

Anlage
zur Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. November 2014

Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern

Katalog von Anforderungen:

Im Zuge der Umsetzung des Krebsregistergesetzes und Krebsfrüherkennungsgesetzes in den Ländern werden neue Übermittlungswege zwischen verschiedenen medizinischen Leistungserbringern und den klinischen Krebsregistern (KKR) erforderlich. Auf diesen Wegen werden Daten unterschiedlichen Schutzbedarfs transportiert. Der überwiegende Teil von ihnen kann jedoch als hoch sensibel eingeschätzt werden.

Mit dem folgenden Anforderungskatalog sollen Maßnahmen skizziert werden, die einzusetzen sind, um Vertraulichkeit, Authentizität und Integrität der Daten, aber auch die Integrität der eingesetzten Systeme zu gewährleisten. Insgesamt muss ein Schutzniveau erreicht werden, dass dem der Gesundheits-Telematikinfrastruktur gemäß §§ 291a, 291b Strafgesetzbuch (SGB) V entspricht.

Folgende Szenarien können nach den Risiken, die ihnen innewohnen, differenziert werden:

Szenario 1: Die **Meldung** von Daten, die von den klinischen Krebsregistern gemäß § 65c Absatz 1 Satz 1 Nummer 1 SGB V zu erfassen sind.

Szenario 2: Die **patientenbezogene Rückmeldung** von Auswertungsergebnissen im Sinne von Nummer 3.01 des Gesetzlichen Krankenversicherungs(GKV)-Förderkatalogs im Hinblick auf die Aufgabe der KKR gemäß § 65c Absatz 1 Satz 1 Nummer 2 SGB V.

Szenario 3: Die **aggregierten Rückmeldungen** an die Leistungserbringer, soweit die übertragenen Daten einen Bezug zu einzelnen behandelnden Personen aufweisen.

Szenario 4: Die **Bereitstellung** von patientenbezogenen Dokumentationsdaten für Zwecke der einrichtungsübergreifenden Behandlung, insbesondere für Tumorkonferenzen im Hinblick auf die Aufgabe der KKR gemäß § 65c Absatz 1 Satz 1 Nummer 4 SGB V.

Im Weiteren wird bei jeder Anforderung auf die Szenarien, auf die sie anwendbar sind, mit ihrer Nummer hingewiesen. Wo erforderlich wird eine zusätzliche Unterscheidung zwischen nachrichtenbasierten Übermittlungsverfahren und webbasierten Dialogverfahren getroffen, worauf durch Zusatz der Buchstaben N beziehungsweise W hingewiesen wird.

Nachrichtenbasierte versus dialogbasierte Übermittlung

1. Vorzugswürdige Form der Übermittlung ist die Lieferung verschlüsselter strukturierter Dateien, wie sie derzeit bei der Meldung der Klinikregister an eine Reihe von epidemiologischen Registern praktiziert wird. Die verschlüsselten Dateien können dabei auch per Web-Upload beziehungsweise Web-Download übertragen werden. Leistungser-

bringer benötigen für diese Übermittlungsvariante ein Krankenhausinformationssystem (KIS) beziehungsweise Praxisverwaltungssystem (PVS), das einen Datenexport in dem vom KKR vorgegebenen Format ermöglicht, oder eine Software zur dezentralen Datenerfassung, die von dem KKR bereitgestellt werden könnte. Die Verschlüsselung beziehungsweise Entschlüsselung und die Signatur der Daten beziehungsweise die Signaturprüfung kann durch separate Software realisiert werden, die kostenfrei erhältlich ist. Investitionen für eine Anpassung von Netzen und Systemen der Leistungserbringer werden in dieser Variante voraussichtlich nur in geringem Maße erforderlich. Die Anforderungen an die Transportsicherheit und die Sicherheit der Systeme und Netze, die ausschließlich mit verschlüsselten Daten in Berührung kommen, liegen auf normalem, nicht erhöhtem Niveau. (Szenarien 1N-4N)

2. Eine Übermittlung von Daten zwischen meldenden Leistungserbringern und klinischen Krebsregistern in einem webbasierten Dialogverfahren steht erheblich größeren Schwierigkeiten gegenüber. Für Szenario 1 liegen praktische Erfahrungen aus der epidemiologischen Krebsregistrierung vor, die sich allerdings nur auf eine Erhebung pseudonymisierter Daten beziehen. Von einer Umsetzung für das mit besonders hohen Risiken verbundene Szenario 4 wird dagegen dringend abgeraten.

   Leistungserbringer können bei dieser Variante zwar KIS beziehungsweise PVS verwenden, die nicht für Zwecke der Kommunikation mit den KKR angepasst wurden. Jedes für den Zugriff auf die Webanwendung des KKR verwendete System des Leistungserbringers muss jedoch besonders gesichert und in einem Netzabschnitt betrieben werden, der gleichzeitig den Sicherheitsansprüchen für die Verarbeitung von klaren Patientendaten und für eine Anbindung an dedizierte medizinische Netze genügt, vergleiche hierzu den Beschluss des Düsseldorfer Kreises vom 4./5. Mai 2011 zu Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze. Soweit nicht bereits ein hierfür geeigneter Netzaufbau vorliegt, sind nennenswerte Aufwendungen bei den Leistungserbringern zu tätigen.

   Ferner sind hohe (Szenarien 1-2) bis sehr hohe (Szenario 4) Anforderungen an die Sicherheit der auf Seiten des KKR beteiligten Systeme zu ergreifen, die bei der Ausgestaltung des Dialogsystems und bei dessen Anbindung an das Backend zu berücksichtigen sind. Eine nachträgliche Anpassung eines bestehenden Systems, dessen Design nicht von vornherein auf die besonderen Sicherheitsanforderungen dieses Einsatzumfeldes ausgerichtet wurde, erscheint wenig erfolgversprechend. (Szenarien 1W, 2W, 4W)

3. Die Anwendung weiterer Übermittlungsverfahren, deren Anwendung bisher noch nicht in Betracht gezogen wurde, ist möglich. Sie bedürfen jedoch einer eigenen Risikoanalyse. Als Beispiel sei eine direkte Übermittlung von Meldedaten aus dem KIS beziehungsweise PVS eines Leistungserbringers an das Register über eine von diesem Register angebotene Webschnittstelle und einen gesicherten Kanal genannt. Auch hier wäre Verschlüsselung und Signatur der Inhaltsdaten geboten. Würde dieses Verfahren auch für den Abruf verwendet, entsprächen die Risiken weitgehend denen des webbasierten Dialogverfahrens. Darüber hinaus wäre der Gewährleistung der Integrität des abrufenden Systems besondere Aufmerksamkeit zu widmen.

Vertrauensdienste, kryptografische Algorithmen und Verfahren

4. Die verwendeten kryptografischen Algorithmen und Verfahren müssen eine langfristige Sicherheit gewähren und dem Katalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI)-TR 03116-1 entnommen sein. (Szenarien 1-4)

5. Für die Identifizierung der Teilnehmer des Verfahren, die zu verwendenden Authentisierungsmittel, deren Ausgabe, Anwendung und Rückruf sowie die Schlüsselspei-

cherung sind mindestens die Anforderungen des Schutzniveaus hoch+ gemäß Abschnitten 3 und 4 der BSI-TR 03107-1 zu erfüllen. (Szenarien 1-4)

6. *(optional)* Für Übermittlung, Authentisierung und Verschlüsselung sollen Verfahren der Telematikinfrastruktur nach § 291b SGB V verwendet werden, sobald diese verfügbar sind. (Szenarien 1-4)

7. Die Wurzel der zur Zertifizierung von Teilnehmer-Schlüsseln und KKR-Schlüsseln verwendeten Public-Key-Infrastruktur (PKI) ist allen Beteiligten integritätsgeschützt zur Verfügung zu stellen. Die Revokation von öffentlichen Schlüsseln bei Kompromittierung der zugeordneten privaten Schlüssel muss unverzüglich in einem im Vorhinein festgelegten Zeitrahmen erfolgen. (Szenarien 1-4)

Maßnahmen zum Vertraulichkeitsschutz während des Transports der Daten

8. Bei jeder Übermittlung ist eine Ende-zu-Ende-Verschlüsslung einzusetzen. (Szenarien 1-4)

9. Bei Übermittlungen an KKR sind Schlüssel einzusetzen, deren Authentizität die sendende Stelle zweifelsfrei feststellen kann. (Szenario 1)

10. Bei Übermittlungen an Leistungserbringer sind zertifizierte personenspezifische oder leistungserbringerspezifische Schlüssel einzusetzen. (Szenarien 2-4)

11. Übermittlungen zu und von den klinischen Krebsregistern sollen über besonders geschützte medizinische Netze abgewickelt werden, bei webbasierten Verfahren ist dies zwingend erforderlich. (Szenarien 1-4)

12. Die erfolgreiche Authentisierung des KKR muss für die meldenden beziehungsweise abrufenden Personen klar erkennbar sein. (Szenarien 1W-4W)

13. Es dürfen ausschließlich behandelnde Ärztinnen und Ärzte sowie Personen, die bei ihnen oder in einem behandelnden Krankenhaus als berufsmäßige Gehilfen tätig sind, personenbezogene Abrufe tätigen. (Szenarien 2+4)

14. Im Zuge eines Datenabrufs müssen sich die abrufenden Personen in analoger Anwendung der Regelungen des § 291a Absatz 3 Satz 1 Nummer 4 SGB V zum Zugriff auf Daten mit einer Zwei-Faktor-Lösung authentifizieren. Der elektronische Heilberufeausweis ist hierfür geeignet. (Szenarien 2W+4W)

15. Die Registrierung der Leistungserbringer muss durch die KKR selbst oder durch Stellen vorgenommen werden, die von den Ländern in analoger Anwendung von § 291a Absatz 5c SGB V bestimmt wurden. (Szenarien 2-4)

16. Das System, das zur Bereitstellung der Daten für die Rückmeldung von Auswertungsergebnissen an die Leistungserbringer verwendet wird, muss sicherstellen, dass Rückmeldungen mit Daten eines Patienten oder einer Patientin nur für solche Leistungserbringer bereitgestellt werden, die bezüglich dieses Patienten beziehungsweise dieser Patientin eine Meldung abgegeben haben, und nur dann, wenn kein Widerspruch der Betroffenen vorliegt. (Szenario 2)

17. Aggregierte Auswertungsergebnisse, die sich auf einzelne behandelnde Personen beziehen, dürfen nur an diese selbst beziehungsweise an die Stellen übermittelt werden, bei denen sie tätig sind. (Szenario 3)

18. Abrufe von Daten müssen auf der Grundlage eines Berechtigungskonzeptes autorisiert werden, mit dem sichergestellt wird, dass nur an der Behandlung der jeweiligen betroffenen Person beteiligte Leistungserbringer Zugang zu den Daten über diese Person erhalten. Das Bestehen des Abrufrechts ist auf die Dauer der Behandlung zu beschränken. Soweit landesrechtlich vorgesehen, muss das Berechtigungskonzept

vorsehen, dass Willenserklärungen der Betroffenen, die auf die Einschränkung der Offenbarung ihrer Daten gerichtet sind, effektiv berücksichtigt werden können. (Szenario 4)

Maßnahmen zum Vertraulichkeitsschutz gespeicherter Daten und zur Gewährleistung der Integrität der beteiligten IT-Systeme

19. Ambulante Leistungserbringer müssen die „Empfehlungen zu Datenschutz und Datensicherheit in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung beachten. Hierauf ist bei der Registrierung hinzuweisen. (Szenarien 1-4)

20. Die Verschlüsselung der zu meldenden und die Entschlüsselung der von einem klinischen Krebsregister abgerufenen Daten darf nur auf Geräten erfolgen, die zur allgemeinen Verarbeitung von Patientendaten der Leistungserbringer vorgesehen sind. (Szenarien 1-4)

21. Hierzu gehört, dass von den zu Meldung oder Abruf genutzten Geräte dann kein allgemeiner Zugang zu Diensten des Internets möglich sein darf, wenn unverschlüsselte Patientendaten auf ihnen zur Anzeige gebracht oder gespeichert werden. (Szenarien 1-4)

22. Bei den KKR sind für die Server, welche zur Abwicklung der Übermittlungen eingesetzt werden, Informationssicherheitsmaßnahmen zu treffen, die bei ausschließlicher Verarbeitung verschlüsselter Daten dem normalen, sonst dem besonders hohen Schutzbedarf der zu übermittelnden Daten gerecht werden. Dies schließt die Maßnahmen nach den Grundschutzbausteinen des Bundesamtes für Sicherheit in der Informationstechnik, insbesondere nach Baustein B 5.21 der Grundschutzkataloge, und die in der ISi-Reihe (BSI-Standard zur Internetsicherheit) empfohlenen Maßnahmen ein. (Szenarien 1-4)

23. Bei Dialogverfahren sind die dort aufgeführten Maßnahmen jedoch nicht notwendig ausreichend. Es wird eine besonders eingehende Risikoanalyse erforderlich, die sich auf alle beteiligten Systeme erstrecken und alle bekannten Angriffsvektoren, die gegenwärtig hohe Angriffsintensität auf Webanwendungen sowie darüber hinaus aufgrund einschlägiger Erfahrung der Vergangenheit die Kompromittierung einzelner Sicherheitsvorkehrungen berücksichtigen muss (defense in depth). (Szenarien 1W-4W)

24. Die Sicherung hat alle OSI-Netzebenen einschließlich der Anwendungsebene zu berücksichtigen. Nur im Vorhinein autorisierten Systemen ist der Aufbau einer Verbindung zu ermöglichen. Diese Beschränkung muss kryptografisch durchgesetzt werden; eine Beschränkung auf Basis von IP-Adressen reicht nicht aus. Die Absicherung mittels Transport Layer Security (TLS, deutsch Transportschichtsicherheit) allein bietet aufgrund der Häufigkeit und Schwere der in der vergangenen Zeit aufgetretenen Schwachstellen keine ausreichenden Garantien für die Sicherheit des Zugriffs. (Szenarien 1W-4W)

25. Die Integrität der Komponenten für die Bereitstellung eines Webdienstes (Webserver, Anwendungsserver, Datenbank) bedürfen besonderen Integritätsschutzes. Eine direkte Anbindung an das Datenhaltungssystem des Registers in der inneren Sicherheitszone ist nicht zulässig. Die Datenhaltung des Backends der Webanwendung ist nur verschlüsselt zulässig. (Szenarien 1W-4W)

26. Kryptografische Schlüssel, deren Kenntnis für den Zugriff auf den Datenbestand erforderlich ist, sind in dedizierten Systemen hardwareseitig zu kapseln und ihre Nutzung durch ein Intrusion Prevention System zu überwachen. Ungewöhnliche Nutzungsmuster müssen zu einer Unterbrechung der Nutzungsmöglichkeiten und einer Untersuchung des Sicherheitsstatus des Verfahrens führen. Kryptografische Schlüssel, die in

der inneren Sicherheitszone des Registers verwendet werden, dürfen innerhalb der Webanwendung nicht genutzt werden. (Szenario 4W)

Maßnahmen zur Gewährleistung der Authentizität der Daten

27. Da die übermittelten Daten einer folgenden Behandlung zugrunde gelegt werden können, ist es erforderlich, die Integrität der Daten während ihrer Übermittlung zu schützen und sicherzustellen, dass die Daten stets ihrem Ursprung zuzuordnen sind. (Szenarien 1+4)

28. Nachrichten der Leistungserbringer mit Krebsregisterdaten sind entweder mit einer personenbezogenen mindestens fortgeschrittenen elektronischen Signatur oder leistungserbringerbezogen mit einem mindestens fortgeschrittenen elektronischen Siegel im Sinne von Artikel 3 Nummer 26 der EU-Verordnung 910/14 zu authentisieren. (Szenarien 1+4)

Maßnahmen zur Transparenz und Datenschutzkontrolle

29. Abrufe sind leistungserbringerbezogen und personenbezogen zu protokollieren. Die Protokolle sind mindestens ein Jahr zu speichern. Sie müssen gegen Veränderung geschützt werden. (Szenarien 2-4)

30. Für die Protokolle ist ein Verfahren zur anlassbezogenen Auswertung vorzuhalten. (Szenarien 2-4)

31. Der Inhalt der Protokolldaten ist bezogen auf Abrufe von Daten einer Patientin oder eines Patienten auf deren Antrag zu beauskunften. (Szenario 4)

Um einen datenschutzgerechten Betrieb der Verfahren der klinischen Krebsregister für die Kommunikation mit den Leistungserbringern zu gewährleisten, wird den verantwortlichen Stellen der Länder empfohlen, die vorgenannten Anforderungen bereits bei der Ausschreibung von Leistungen zur Bereitstellung der von den KKR benötigten Informationstechnik zu berücksichtigen.

19.14 Schluss mit den datenschutzrechtlichen Missständen beim Umgang mit Krankengeldbeziehern!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. Dezember 2014)

Bei dem derzeit praktizierten „Krankengeldfallmanagement“ lädt eine Vielzahl von Krankenkassen ihre Versicherten in der vierten Woche einer Arbeitsunfähigkeit zu einem persönlichen Gespräch ein. Die Krankenkassen stellen Fragen zur Arbeitsplatz-, Krankheits-, familiären und sozialen Situation des Versicherten. Außerdem sollen die Ärzte der Versicherten häufig medizinische Fragen beantworten sowie Arzt-, Krankenhaus- oder Reha-entlassungsberichte an die Krankenkasse schicken. Vielfach werden Versicherte, die im Krankengeldbezug stehen – zum Teil mehrfach wöchentlich – von Krankenkassenmitarbeitern oder in deren Auftrag von Dritten angerufen, um sich nach dem Fortschritt der Genesung zu erkundigen.

Zudem werden nach den Prüferfahrungen der Datenschutzbeauftragten des Bundes und einiger Länder Versicherte beim „Krankengeldfallmanagement“ von ihrer Krankenkasse oftmals unter Druck gesetzt. Auch der Patientenbeauftragte der Bundesregierung sowie die Unabhängige Patientenberatung Deutschland (UPD) haben an dieser Praxis starke Kritik geübt.

Die Krankenkassen sind zur Beurteilung sensibler medizinischer Daten aufgrund der bisherigen gesetzgeberischen Grundentscheidung auf ein Tätigwerden des Medizinischen Dienstes der Krankenversicherung (MDK) angewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist die Bundesregierung darauf hin, dass es nicht nachvollziehbar ist, dass mit dem Entwurf eines Gesetzes zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKV-Versorgungsstärkungsgesetz – GKV-VSG) das bisherige datenschutzrechtlich problematische Vorgehen von vielen Krankenkassen beim sogenannten Krankengeldfallmanagement nunmehr legitimiert werden soll. Zukünftig sollen danach die Versicherten bei einem (absehbaren) Krankengeldbezug „Anspruch auf eine umfassende Prüfung, individuelle Beratung und Hilfestellung, welche Leistungen und unterstützende Angebote zur Wiederherstellung der Arbeitsfähigkeit erforderlich sind“ gegenüber ihrer gesetzlichen Krankenkasse haben. Die Krankenkasse soll dabei die erforderlichen personenbezogenen Daten mit Einwilligung des Versicherten erheben, verarbeiten und nutzen dürfen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, von dieser Regelung Abstand zu nehmen. Vielmehr sind die derzeit bestehenden gesetzlichen Regelungen konsequent umzusetzen.

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

20.1 Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sogenannte Dashcams)

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 25./26. Februar 2014)

Mittlerweile nimmt der Einsatz sogenannter Dashcams auch in Deutschland immer mehr zu, um, so die standardmäßige Begründung, im Falle eines Unfalls den Hergang nachvollziehen und das Video gegebenenfalls als Nachweis bei der Regulierung von Schadensfällen und der Klärung von Haftungsfragen heranziehen zu können.

Die Aufsichtsbehörden des Bundes und der Länder für den Datenschutz im nicht öffentlichen Bereich machen darauf aufmerksam, dass der Einsatz solcher Kameras – jedenfalls sofern dieser nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt – datenschutzrechtlich unzulässig ist.

Soweit mit den Dashcams in öffentlich zugänglichen Bereichen gefilmt wird und als Hauptzweck der Aufnahmen die Weitergabe von Filmaufnahmen zur Dokumentation eines Unfallhergangs angegeben wird, ist der Einsatz – auch wenn die Kameras von Privatpersonen eingesetzt werden – an den Regelungen des Bundesdatenschutzgesetzes zu messen. Gemäß § 6b Absatz 1 Nummer 3 und Absatz 3 des Bundesdatenschutzgesetzes (BDSG) ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Diese Voraussetzungen sind in aller Regel nicht erfüllt, da die schutzwürdigen Interessen der Verkehrsteilnehmer überwiegen. Das informationelle Selbstbestimmungsrecht umfasst das Recht des Einzelnen, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Dashcams zeichnen den Verkehr sowie Personen, die sich in der Nähe einer Straße aufhalten, ohne Anlass und permanent auf, sodass eine Vielzahl von Verkehrsteilnehmern betroffen ist, die sämtlich unter einen Generalverdacht gestellt werden, ohne dass sie von der Überwachung Kenntnis erlangen oder sich dieser entziehen können. Das Interesse des Autofahrers, für den eher theoretischen Fall eines Verkehrsunfalls Videoaufnahmen als Beweismittel zur Hand zu haben, kann diesen gravierenden Eingriff in das Persönlichkeitsrecht der Verkehrsteilnehmer nicht rechtfertigen.

Da selbst die Polizei Videokameras zur Verfolgung von Straftaten und Ordnungswidrigkeiten nur auf der Grundlage spezifischer Regelungen und ausschließlich dann einsetzen darf, wenn gegen die betroffene Person ein entsprechender Anfangsverdacht besteht, können erst recht sonstige Stellen nicht für sich beanspruchen, den öffentlichen Verkehrsraum anlasslos und schrankenlos mittels Kameras zu überwachen.

20.2 Modelle zur Vergabe von Prüfzertifikaten, die im Wege der Selbstregulierung entwickelt und durchgeführt werden

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 25./26. Februar 2014)

I. Ausgangslage

Freiwillige Audits leisten einen bedeutenden Beitrag für den Datenschutz, weil sie als aus eigenem Antrieb veranlasste Maßnahme die Chance in sich bergen, zu mehr Datenschutz in der Fläche zu gelangen.

Datenschutz sollte ein Wettbewerbsvorteil sein. Unternehmen, die sich um einen hohen Datenschutzstandard bemühen, möchten dies auch anerkannt sehen. Ein Datenschutzzertifikat ist ein wichtiges Signal an diese Unternehmen.

Zugleich trägt ein Zertifikat dazu bei, das Vertrauen von Bürgerinnen und Bürgern, Verbraucherinnen und Verbraucher in den achtsamen Umgang mit ihren Daten zu fördern.

Eigenverantwortung ist eine wichtige Säule für einen funktionierenden Datenschutz.

Der Ruf nach einem Audit hat im Zuge der Diskussion um den europäischen Rechtsrahmen weiteren Auftrieb erhalten. Initiativen auf Landesebene und nunmehr auch auf Bundesebene haben dieses Anliegen aufgegriffen.

II. Erprobung von Modellen, Anforderungen

Die Gesetzgeber haben bisher lediglich einzelne Teilregelungen zu Zertifizierungen getroffen.

Der Düsseldorfer Kreis unterstützt weitergehende Bemühungen, Erfahrungen mit Zertifizierungen zu sammeln, die in eigener Verantwortung im Wege der Selbstregulierung auf der Grundlage von Standards erfolgen, die die Aufsichtsbehörden befürworten.

Verlässliche Aussagen für Bürgerinnen und Bürger, für Verbraucherinnen und Verbraucher erfordern, dass Zertifizierungsdienste anbietende Stellen (Zertifizierungsdienste) geeignete inhaltliche und organisatorische Vorkehrungen für derartige Verfahren mit dem Ziel treffen, eine sachgerechte und unabhängige Bewertung zu gewährleisten.

Dazu gehören im Kern folgende, von Zertifizierungsdiensten zu bearbeitende Strukturelemente:

— Prüffähige Standards, die von den Aufsichtsbehörden befürwortet werden, zu entwickeln, zu veröffentlichen und zur Nutzung für Dritte freizugeben,

— beim Zertifizierungsprozess zwischen verschiedenen Ebenen zu unterscheiden (Prüfung, Zertifizierung, Akkreditierung),

— für verschiedene auf Ebenen und/oder in Verfahrensabschnitten anfallende Aufgaben voneinander abzugrenzende Rollen der jeweils Mitwirkenden vorzusehen,

— Regelungen zur Vermeidung von Interessenkollisionen der an einem Zertifizierungsprozess Beteiligten zu treffen,

— Anforderungen an die Eignung als Prüferin und Prüfer festzulegen und diesen Personenkreis für Zertifizierungen zu qualifizieren,

— den geprüften Sachbereich so zu umschreiben, dass Bürgerinnen und Bürger, Kundinnen und Kunden die Reichweite der Prüfaussage ohne weiteres dem Zertifikat entnehmen können,

— Bedingungen für Erteilung, Geltungsdauer und Entzug von Zertifikaten zu bestimmen,

— Zertifikate zusammen mit den wesentlichen Ergebnissen der Prüfberichte zu veröffentlichen.

III. Abstimmung im Düsseldorfer Kreis

Der Düsseldorfer Kreis verfolgt die Entwicklung von sowohl auf Landesebene mit dieser Zielrichtung begleiteten Initiativen als auch auf Bundesebene begonnenen weiteren Initiativen. Er beteiligt sich an einer ergebnisoffenen Diskussion, um zu optimalen Verfahrensgestaltungen zu gelangen.

Die im Düsseldorfer Kreis zusammenwirkenden Aufsichtsbehörden sehen daher als gemeinsame Aufgabe, sich auf inhaltliche und verfahrensmäßige Anforderungen für Zertifizierungsverfahren zu verständigen und zu Beratungsersuchen im Interesse einer bundesweit einheitlichen Aufsichtspraxis auf im Düsseldorfer Kreis abgestimmter Grundlage Stellung zu nehmen.

20.3 Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 23./24. September 2014)

Der Düsseldorfer Kreis weist auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen. Die Datenverarbeitung in modernen Fahrzeugen schafft Begehrlichkeiten, die dort anfallenden Daten für die verschiedensten Zwecke nutzen zu wollen – etwa bei Arbeitgebern und Versicherungen. Dabei besteht die Gefährdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergeräten und nicht erst mit deren Auslesen oder Übermitteln. Bereits diese personenbezogenen Daten geben Auskunft über Fahrverhalten und Aufenthaltsorte und können zur Informationsgewinnung über den Fahrer beziehungsweise den Halter bis hin zur Bildung von Persönlichkeitsprofilen herangezogen werden.

Um eine selbstbestimmte Fahrzeugnutzung frei von Furcht vor Überwachung zu gewährleisten, sind Automobilhersteller, Händler, Verkäufer, Werkstätten ebenso wie Anbieter von Kommunikationsdiensten und Telediensten rund um das Kraftfahrzeug im Rahmen ihres Wirkungskreises in der Pflicht, informationelle Selbstbestimmung im und um das Kraftfahrzeug zu gewährleisten.

Dazu gehört:

— Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote für Kommunikationsdienste und Teledienste die Datenschutzgrundsätze von Privacy-by-Design beziehungsweise Privacy-by-Default zu verwirklichen.

— Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zugrunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.

— Die Datenverarbeitungen müssen entweder vertraglich vereinbart sein oder sich auf eine ausdrückliche Einwilligung stützen.

— Für Fahrer, Halter und Nutzer von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden. Änderungen sind rechtzeitig anzuzeigen. Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzer ebenfalls zu informieren.

— Auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübermittlung an den Hersteller oder sonstige Diensteanbieter sind Fahrer, Halter und Nutzer technisch und rechtlich in die Lage zu versetzen, Datenübermittlungen zu erkennen, zu kontrollieren und gegebenenfalls zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.

— Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und Datenintegrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.

Auf dieser Grundlage wirken die Datenschutzaufsichtsbehörden darauf hin, dass Automobilhersteller, Zulieferer und ihre Verbände bundesweit einheitliche Datenschutzstandards auf hohem Niveau setzen, die dazu beitragen, dass Innovation auch mit gesellschaftlicher Akzeptanz einhergeht.

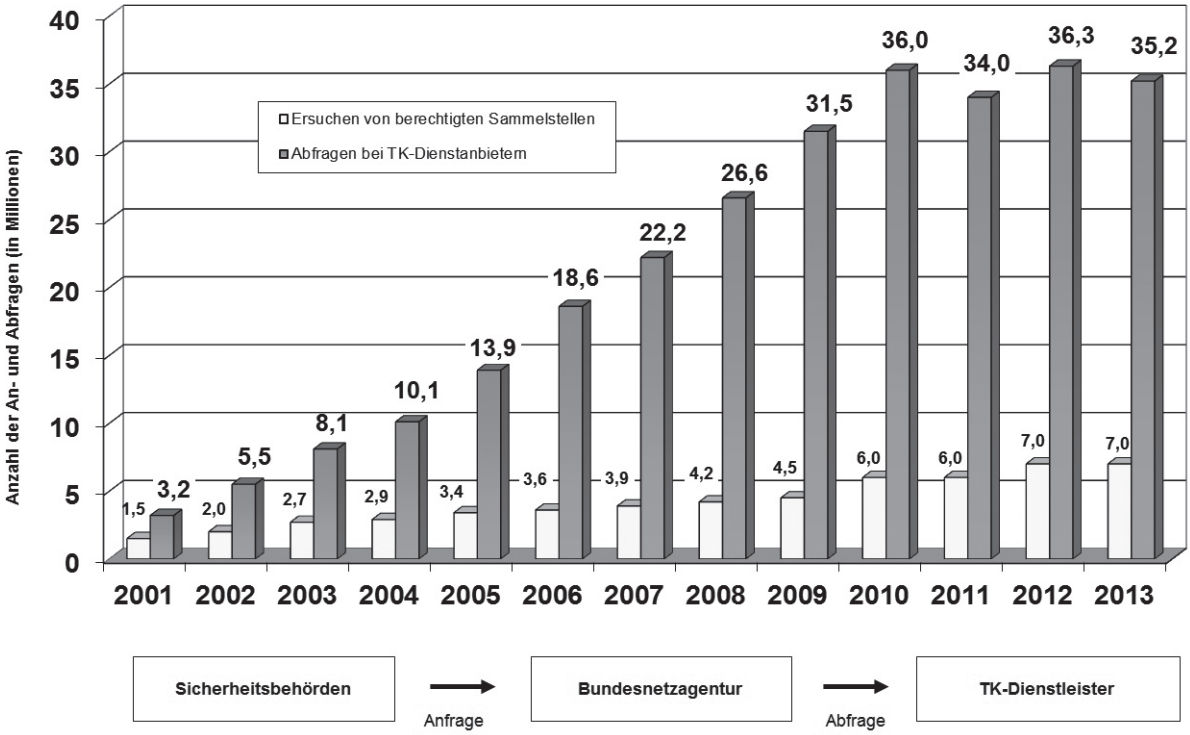
21. Die europäische und die internationale Datenschutzkonferenz

Die Entschließungen der europäischen Datenschutzkonferenz im Jahr 2014 sowie Informationen zu den Entschließungen der internationalen Datenschutzkonferenz stehen auf der Seite der Bundesbeauftragten für den Datenschutz und für die Informationsfreiheit unter http://www.bfdi.bund.de/DE/Infothek/Entschliessungen/entschliessungen-node.html zur Verfügung.

22. Anhang

22.1 Automatisierte Auskunftsverfahren gemäß § 112 Telekommunikationsgesetz

Sicherheitsbehörden erhalten gemäß § 112 Telekommunikationsgesetz (TKG) über die Bundesnetzagentur von Telekommunikationsdiensteanbietern Auskünfte aus deren Kundendateien (Namen und Anschriften der Inhaber von Rufnummern). Derzeit erhalten etwa 200 berechtigte Stellen und mehrere tausend hieran angeschlossene Abfragestellen der Strafverfolgungsbehörden automatisiert entsprechende Bestandsdaten bei circa 140 Telekommunikationsdiensteanbietern.



Quelle: Jahresbericht 2013 der Bundesnetzagentur

22.2 Liste des verfügbaren Informationsmaterials

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

22.3 Index

Druck: Anker-Druck Bremen